FRAMEWORK FOR SECURITY TRANSPARENCY IN CLOUD COMPUTING

Umar Mukhtar Ismail

A thesis submitted in partial fulfilment of the requirements of the University of East London for the degree of Doctor of Philosophy

January 2020

Abstract

The migration of sensitive data and applications from the on-premise data centre to a cloud environment increases cyber risks to users, mainly because the cloud environment is managed and maintained by a third-party. In particular, the partial surrender of sensitive data and application to a cloud environment creates numerous concerns that are related to a lack of security transparency. Security transparency involves the disclosure of information by cloud service providers about the security measures being put in place to protect assets and meet the expectations of customers. It establishes trust in service relationship between cloud service providers and customers, and without evidence of continuous transparency, trust and confidence are affected and are likely to hinder extensive usage of cloud services. Also, insufficient security transparency is considered as an added level of risk and increases the difficulty of demonstrating conformance to customer requirements and ensuring that the cloud service providers adequately implement security obligations.

The research community have acknowledged the pressing need to address security transparency concerns, and although technical aspects for ensuring security and privacy have been researched widely, the focus on security transparency is still scarce. The relatively few literature mostly approach the issue of security transparency from cloud providers' perspective, while other works have contributed feasible techniques for comparison and selection of cloud service providers using metrics such as transparency and trustworthiness. However, there is still a shortage of research that focuses on improving security transparency from cloud users' point of view. In particular, there is still a gap in the literature that (i) dissects security transparency from the lens of conceptual knowledge up to implementation from organizational and technical perspectives and; (ii) support continuous transparency by enabling the vetting and probing of cloud service providers' conformity to specific customer requirements. The significant growth in moving business to the cloud – due to its scalability and perceived effectiveness – underlines the dire need for research in this area.

This thesis presents a framework that comprises the core conceptual elements that constitute security transparency in cloud computing. It contributes to the knowledge domain of security transparency in cloud computing by proposing the following. Firstly, the research analyses the basics of cloud security transparency by exploring the notion and foundational concepts that constitute security transparency. Secondly, it proposes a framework which integrates various concepts from requirement engineering domain and an accompanying process that could be followed to implement the framework. The framework and its process provide an essential set of conceptual ideas, activities and steps that can be followed at an organizational level to attain security transparency, which are based on the principles of industry standards and best practices. Thirdly, for ensuring continuous transparency, the thesis proposes an essential tool that supports the collection and assessment of evidence from cloud providers, including the establishment of remedial actions for redressing deficiencies in cloud provider practices. The tool

serves as a supplementary component of the proposed framework that enables continuous inspection of how predefined customer requirements are being satisfied.

The thesis also validates the proposed security transparency framework and tool in terms of validity, applicability, adaptability, and acceptability using two different case studies. Feedbacks are collected from stakeholders and analysed using essential criteria such as ease of use, relevance, usability, etc. The result of the analysis illustrates the validity and acceptability of both the framework and tool in enhancing security transparency in a real-world environment.

Dedication

To my parents, without whom this research wouldn't have been possible

Acknowledgement

The researcher wishes to acknowledge and express his gratitude to several professionals whose contributions invaluable contribution made this research a reality. Others are family and friends who have provided motivation and inspiration.

From an academic point of view, my sincere gratitude goes to my supervisor, Dr Shareeful Islam, for guiding me through this research work with immeasurable knowledge, suggestions, encouragement and support.

I also wish to express my profound appreciation to Mr Kingsley Austin and Mohammed Hossain for giving me the platform to evaluate my research. Also, a million thanks are due to the stakeholders in the case-study organisations who took part in the implementation of my work and the provision of feedback.

I wish to express my sincere gratitude and appreciation to my fiancée, who had been with me through all the trials and tribulations, taking emotional sacrifices to see the completion of my PhD, also, to my friend-sister, Halima Ibrahim Kure whose support and encouragement is profoundly appreciated.

Table of Contents

List of publication

- Towards Cloud Security Monitoring: A Case Study. IEEE Cyber Security and Cyberforensics Conference (2016).
- A Framework for Security Transparency in Cloud Computing. Future Internet Journal on Internet Technologies and Information Society (2016)
- A Framework for Cloud Security Audit. International Conference on Global Security, Safety and Sustainability (2015).
- Cloud Security Audit for Migration and Continuous Monitoring. IEEE Trust, Security and Privacy in Computing and Communications, IEEE International Conference (2015)

List of Tables

List of Figures

List of Abbreviations

Acronyms	Terms
API	Application Programming Interface
CAIQ	Consensus Assessment Initiative Questionnaire
CC	Cloud Customer
CCM	Cloud Control Matrix
CIA	Confidentiality, Integrity and Availability
CIS CSC	Centre for Internet Security Critical Security Controls
CPU	Central Processing Unit
CSA	Cloud Control Matrix
CSP	Cloud Service Provider
CSTF	Cloud Security Transparency Framework
CU	Cloud User
DREAD	Damage, Reproducibility, Explorability, Affected Users, Discoverability
ECM	Enterprise Content Management
ECM	Document Management Solution
ENISA	European Union Agency for Network and Information Security
IaaS	Infrastructure as a Service
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
ISAE	International Standard on Assurance Engagements
ISMS	Information Security Management Systems
ISO	International Standards Organisation
NERC	North American Electric Reliability Cooperation
NIST	National Institute of Standards and Technology
OS	Operating System
OWASP	Open Web Application Security Projects
PaaS	Platform as a Service
PAR	Participatory Action Research
PCI DSS	Payment Card Industry Data Security Standards
PRM	Patient Relationship Manager
RfI	Request for Information
RfP	Request for Proposal
SA	Security Analyst
SaaS	Software as a Service
SCUAR	Sufficiency, Completeness, Understandability, Accuracy and Reliability
SLA	Service Level Agreement
SLR	Systematic Literature Review
SOI	Service-Oriented Infrastructure
START	Security Trust and Assurance Registry
STAT	Security Transparency and Audit Tool
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Duties
VMM	Virtual Machine Manager
XML	Extensible Mark-up Language

CHAPTER ONE

1.0 Introduction

In traditional operating environments, businesses usually procure physical hardware and software resources to deploy IT infrastructure for supporting business goals and objectives, which are often associated with a considerable cost for procurement, maintenance and upgrade (Rittinghouse and Ransome, 2017). But that is no longer the case as many businesses nowadays consider cloud computing as an enabler of business strategy that provides a competitive edge (Marston et al., 2011). This is made possible by the evolution of virtualisation technologies, high-speed networks and the widespread availability of multicore high-performance computing platforms that have substantially created unlimited possibilities for businesses to access higher computing power on a pay-as-you-go basis. As a computational model, cloud computing is fast becoming one of the most rapidly evolved computing paradigm in recent times and is still receiving a lot of attention, owing to the advantages it offers such as high capacity computing, reduced operational cost and enabling endless business transformations (Sun, 2019). Businesses across all industries are continually considering the migration of mission-critical data and applications to cloud-based services to benefit from the multifarious advantages offered by the technology (Garrison et al., 2012).

Despite its benefits, cloud computing comes with numerous challenges that forestall extensive adoption (Bhushan and Gupta, 2017). For example, current studies and literature have cited cloud service providers (CSP) ability to provide adequate security transparency as a significant hindrance to cloud adoption (Kandukuri and Rakshit, 2009, Jouini and Rabai, 2019). This concern could be influenced by the uncertainties surrounding CSPs' use of appropriate practices and processes to deliver reasonable means for satisfying asset security and other requirements, as well as due diligence to promptly inform customers on events relating to security incidents (Kandukuri and Rakshit, 2009). The apprehension over security lapses and lack of visibility on critical operations will continue to hinder broader cloud adoption, particularly for businesses dealing with security-critical data and applications (Ouedraogo et al., 2015b). In a nutshell, there is the need for a systematic approach to help businesses ensure that assets in the cloud environment are sufficiently protected, security events transparently shared to users, while also supporting audibility. Such an assertion arises from the consideration that the processes applied to secure assets are geographically dispersed from customers' premises— a practice that makes transparency highly necessary due to the devolution of security-related responsibilities.

1.1 Statement of the Problem

The migration of mission-critical data to cloud service implies a partial surrender or sharing significant control over security and handling of data. The lack of control over data creates other problems that affect security and privacy of data which are far within reach of cloud computing customers. This is especially the case as customers move their business process or data to the cloud, their risk profile also

changes, and becomes a combination of inherent risks and a subset of the CSPs'(Rao and Selvamani, 2015). As a result, customers of cloud computing service are more concerned about how the CSP is controlling sensitive data, especially if the data is highly critical. This issue is mainly due to lack of transparency, and to some extent, lack of vetting mechanisms by which customers can evaluate CSPs practices and conformance to necessary data security measures once data is migrated to the cloud (Ouedraogo et al., 2015a). What is more worrying is the fall-out effect that is likely to happen from this lax approach to security controls from the CSP side. A recent study of significant security incidents in cloud services by Proofpoint (Proofpoint, 2019) found that 40% of cloud customers have had at least one account compromise and data breach in their environment unreported by the CSP. This example and many more incidents highlight essential concerns such as what security practices are being put in place by the CSP to ensure the safety of customer data? How is the CSP able to show that they are in full compliance with customer requirements? What measures are put in place to ensure that customers get informed of events requiring their prompt attention? (Sun, 2019) (Flittner et al., 2016).

Thus, despite the numerous benefits and rapid acceptance of the cloud computing, three are still pressing challenges that forestall broader acceptance of cloud service, including lack of transparency, accountability, trust and privacy, and deployed controls (Singh and Chatterjee, 2017, Rittinghouse and Ransome, 2016). Several efforts have been proposed in the literature for fostering security transparency. Some of such contributions have recommended purposely developed tools and techniques that serve to aid the selection of CSP before cloud migration takes place. Such contributions include C.A.RE (Ouedraogo and Mouratidis, 2013), SMICloud (Garg et al., 2013), service quality model with provider trustworthiness (Sumetanupap and Senivongse, 2011), Cloud Security Alliance's Trust, and Assurance Registry (STAR) (Cloud Security Alliance, 2015). While a lot of focus centres on addressing transparency issues before customers move data to the cloud, there is still a lack of on-going transparency, particularly on deployed controls and practices of the CSP after cloud migration. As argued by Anisetti et al (Anisetti et al., 2017), transparency can only be achieved when reliable evidence on the behaviour of cloud services, processes and deployed controls are shared and independently verified by customers on continuous basis. Hence, continuous collection and verification of reliable evidence relating to CSP handling of customer and requirements have become paramount for a trustworthy cloud.

In addition, security transparency is still a significant issue as some challenges need to be addressed from the viewpoint of cloud customers. For instance, there is the argument that major CSPs such as Amazon, Google and Rackspace have well documented and publicised security practices. However, the scant security information and evidence available make it difficult for customers to garner enough insight into actual security controls, and to verify the existence of CSP acclaimed processes (A Martin, 2018). This is due to the inadequacy of evidence-based analysis and verification mechanisms, which is perceived to continue as a barrier to customers' trust and prevent customers from taking full

advantage of cloud services (Almorsy et al., 2016). Also, vetting mechanisms (auditing capabilities) that support customers to perform a systematic evaluation to determine the CSPs conformance to predefined requirements is another critical issue.

Security auditing based on relevant company requirements gives customers the ability to identify and probe CSPs visibly: conformity to contractual agreements, data security requirements, and potential issues to assets under the custody of a CSP. Additionally, security auditing enables businesses to have sufficient information in identifying security lapses and assessing the adequacy of CSP security implementations which help in meeting regulatory compliance. However, auditing solutions in the cloud are still lacking and insufficiently developed in assisting businesses to track assets, identify how requirements are being met, or detect the occurrence of security incidents to critical assets.

In this direction, the Cloud Security Alliance introduced the STAR registry system (Cloud Security Alliance, 2015), which aims at documenting the security controls provided by various CSP offerings. CSA STAR comprises the CAIQ questionnaire that organisations and auditors can use to ask CSP questions relating to their security procedures. However, this initiative only supports organisations to consider CSP assertions but does not support evidence-based auditing and probing of CSPs after cloud migration. Further, some CSPs only support limited incident response within their services to assist customers in the containment of incidents that have already occurred and affected critical assets. It could be argued that cloud security controls are not tailored according to user-specific needs, and literature citations (Jouini and Rabai, 2019, Bhushan and Gupta, 2017) have also shown that CSPs usually focus more on controls related to the overall cloud infrastructure rather than specific user needs. Other application-specific techniques used in the traditional client-server model are also used and applied to cloud context but may fall short in different ways.

1.1.1 Research Approach to the Problems

The approach of this thesis is upon the perception that organisations, in general, tend to have less trust and confidence in cloud computing, especially if there is limited disclosure or insufficient information about CSP practices. Unfortunately, cloud services are non-transparent, particularly in certain aspects of operations such as the fulfilment of user expectations. However, this can be mitigated if users are given with adequate assurance that CSPs follow standard practices in mitigating risks, in addition to the provision of adequate insight regarding the conformance to requirements based on verifiable evidence from the CSP. Therefore, in this thesis, it is established that by providing security transparency capabilities at sufficient granularity, a monumental success would be achieved towards addressing salient user concerns relating to trust issues, loss of control and uncertain security guarantees. The research approaches the problem by proposing a systematic framework that aims to help organisations to specify the security requirements relevant for their assets, continuously probe CSP conformance to such security requirements through the collection and analysis of evidence, and establishing of remedial

actions that need to be implemented by the CSP. This approach is considered to not only enhance security transparency but also improve assurance and accountability in cloud computing services.

1.3 Research Questions

The rationale behind this research is to develop a framework that supports organisations to achieve security transparency when using cloud services. A state of the art literature review is carried out to achieve this aim, and essential questions that need answering are identified and summarised as follows:

RQ1: How can security transparency be achieved for assets outsourced to a cloud-based environment?

RQ2: How can organisations migrate assets to the cloud-based on crucial security transparency requirements?

RQ3: How can organisations attain security transparency and assess the fulfilment of crucial asset requirements by probing a CSP?

In responding to the research questions, the research develops a framework that allows a comprehensive understanding of security transparency in cloud computing. It provides a set of interrelated concepts and a process that provide:

i. The fundamental knowledge of cloud transparency and the necessary concepts for attaining security transparency in cloud services.

ii. The integration of security transparency concepts to support cloud customers achieve transparency according to business-related requirements.

iii. A technical perspective of tool support that enables the specification of requirements, collection and assessment of evidence relating to the fulfilment of predefined requirements.

1.4 Research Aims and Objectives

The main aim of this research is to propose and develop a framework that supports security transparency in cloud computing, which will ultimately increase user trust in cloud services. The objectives are given below:

O1: Develop a novel framework that provides users with a solution to achieve security transparency from conceptual, organizational, and technical perspectives.

O2: Propose an implementable security transparency process for cloud migration activities based on the framework, which is formed on the principles of different industry standards.

O3: Develop an assessment tool that enables organisations to collect evidence, and assess CSP's conformance to established requirements, as well as suggesting remedial actions in areas where security improvements are needed

1.5 Research Contributions

In addressing the research problems and questions, the research has taken a stride and made several novel and state of the art contributions. For example, the study has produced a new definition of security transparency as *the disclosure of information relating to the security practices and management of customers resources in the cloud to help them in monitoring, verifying and tracking their assets across cloud infrastructure. Cloud security transparency establishes the trustworthiness of the operations of the CSP by enabling security monitoring, incident detection, reporting and management from the cloud customer's point of view.* In this way, the research has made significant contributions by developing a comprehensive framework that integrates various concepts and process towards establishing security transparency in cloud services. The four novel contributions of this research are listed as:

i. **Contribution 1:** The thesis has addressed some of the challenges associated with cloud security transparency by providing the basics of security transparency in the cloud context. It elaborates what constitutes transparency, its deployment types and practices by using ontological semantics. Considering the insufficient literature that aims at addressing security transparency challenges in the cloud, this contribution improves the state of the art knowledge around security transparency and the means for enabling it.
ii. **Contribution 2:** The research contributes to the current-state-of-the-art knowledge by proposing a security transparency framework. The framework aims at providing a common vocabulary that facilitates the understanding, conceptualisation, and implementation of security transparency from organizational and technical perspectives. It comprises a set of concepts that have been established based on security modelling techniques such as Secure Tropos (Mouratidis and Giorgini, 2007), and formalized using OWL ontologies (Antoniou and Van Harmelen, 2004) to support representation, sharing and reusability of security transparency knowledge. Besides, the framework is accompanied by a process which expresses the conceptual framework into plans, actions and strategies that businesses can follow to accomplish security transparency based on principles of best practices.
iii. **Contribution 3:** The third contribution of this thesis is the development of a tool security transparency and audit tool (STAT). STAT serves as tool support that facilitates the collection and analysis of evidence from the CSP regarding specific user requirements. In other words, STAT helps as an additional component for the proposed framework, which provides a simplified way by which organisations can request for and obtain evidence from CSPs, perform an intelligent assessment of collected evidence for CSP conformance to requirements, and specification of remedial actions using audit decision logics.
iv. **Contribution 4:** The last contribution is the implementation of the framework. The implementation is used to assess the validity and applicability of the framework, its process and

the security transparency tool in supporting real-world organisations to achieve security transparency.

1.6 Thesis Outline

This thesis comprises eight chapters, each focusing on a particular aspect of the research as shown in Figure 1.1

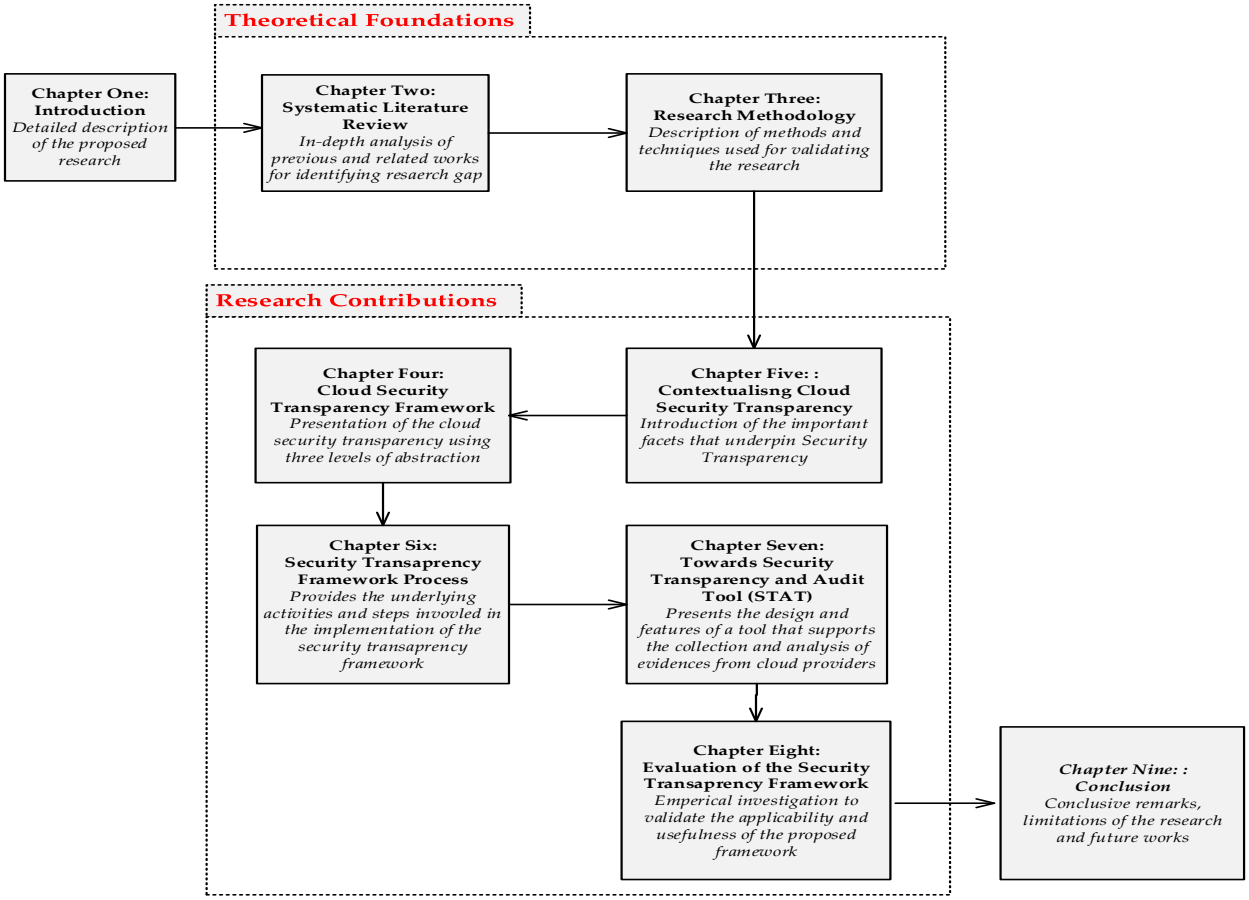

Figure 1.1 Thesis Outline

Chapter One: the thesis starts with the introduction of the research context that provides an understanding of the research area. Research questions are created to guide the identification of research aims, objectives and the contributions of the research towards solving the critical issue.

Chapter Two: provides a review of literature consisting: of a brief overview of the research focus – that is, cloud computing including the benefits it offers and the associated challenges, the underlying

notions that are crucial to the research, and the related works that have been proposed in the area of security transparency.

Chapter Three: presents an overview of the research approach and methodologies deployed to establish the applicability and validity of the proposed framework.

Chapter Four: contextualises and dissects cloud security transparency by providing a new definition, highlighting its basics, principles, categories and deployment practices.

Chapter Five: the main focus of the thesis is discussed - that is, a cloud security transparency framework by providing an in-depth discussion of the different levels of abstraction adopted for the research. The chapter elaborates the method for supporting users in the understanding and alignment of security transparency with the application of ontology-based modelling.

Chapter Six: presents an overview of the underlying process involved in the security transparency framework by introducing different phases of activities that organisations can follow to implement the framework, as well as for understanding cloud adoption process that shifts towards attaining security transparency.

Chapter Seven: presents an overview of the security transparency tool by discussing the architectural design, specifications, and features of the tool.

Chapter Eight: presents an empirical approach used for implementing the proposed framework. The chapter presents the different methods adopted for validating the research.

Chapter Nine: concludes the thesis and provides a comprehensive summary of the proposed approach, with a focus on its practical approach. It also discusses the future directions for the research.

1.7 Chapter Summary

This chapter has introduced the research context in this thesis. In particular, the chapter narrates the problem domain that needs addressing, including the existing measures being used to solve the problems, and how this research proposes to resolve such issues. The chapter also presented essential research questions that have been drawn, which will be answered in the course of the thesis. Besides, the contributions made by the research in addressing the research questions are also presented, and lastly, the outline of the whole thesis is shown in this chapter.

CHAPTER TWO

Literature Review

2.1 Introduction

It is essential to provide a common understanding of the crucial aspects of the research area, including an overview of cloud computing. The primary security issues in cloud computing and the types of controls for addressing these issues are also presented. The chapter also presents related works that are similar to the approach pursued in this work. Hence, the first part of the chapter provides the background of cloud computing. The second part consists of related works that have been conducted in the area of security audit, software agent systems, industry projects and cloud compliance, all of which have similarities with the approach proposed in this research. Also, the review of related works includes a narration of the limitations associated with each technique. The study of literature gives the reader an understanding of existing problems, proposed solutions and weaknesses of the current state of the art in cloud security transparency.

2.2 Overview of Cloud Computing

Cloud computing, as a computational model, is fast becoming one of the most rapidly evolving technology in recent times and is receiving a lot of attention (Oliveira et al., 2014). It is a paradigm that makes it possible to share a pool of configurable resources and achieve on-demand network access such as networks and services (Qian et al., 2009, Zhang et al., 2010). Cloud services have become an integral part of everyday life and have drastically changed how businesses and organisations function. Perhaps, most companies and individuals have resorted to the use of cloud services to support their needs without even realising it. For example, companies nowadays use iCloud, Office 365 and Google Drive for running their day-to-day businesses activities.

The cloud mainly comprises multiple layers of significant infrastructure components that support each other in the delivery of services that are accessible to a large user base. A large number of applications hosted within the cloud infrastructure and the variation of user and application requirements make it highly heterogeneous in structure (Armbrust et al., 2009). Each component provides a different type of service in the cloud. A brief discussion of cloud components is vital to understanding the challenges and differences between deployment and service types.

2.2.1 Cloud Service Models

Cloud service models, also referred to as cloud types in some literature, are architectural models for providing different kinds of services to customers and they can be perceived as a multi-layered

computing architecture where services are built from an underlying layer (Subashini and Kavitha, 2011). As shown in Figure 2.1, the first layer is infrastructure as a service (IaaS) that sits on top of virtualised computing resources. The second layer comprises platform-as-a-service (PaaS) that supports application development and deployment capabilities. While software-as-a-service (SaaS) is built at the top layer to serve as user application level for supporting applications and application programming interfaces (APIs).

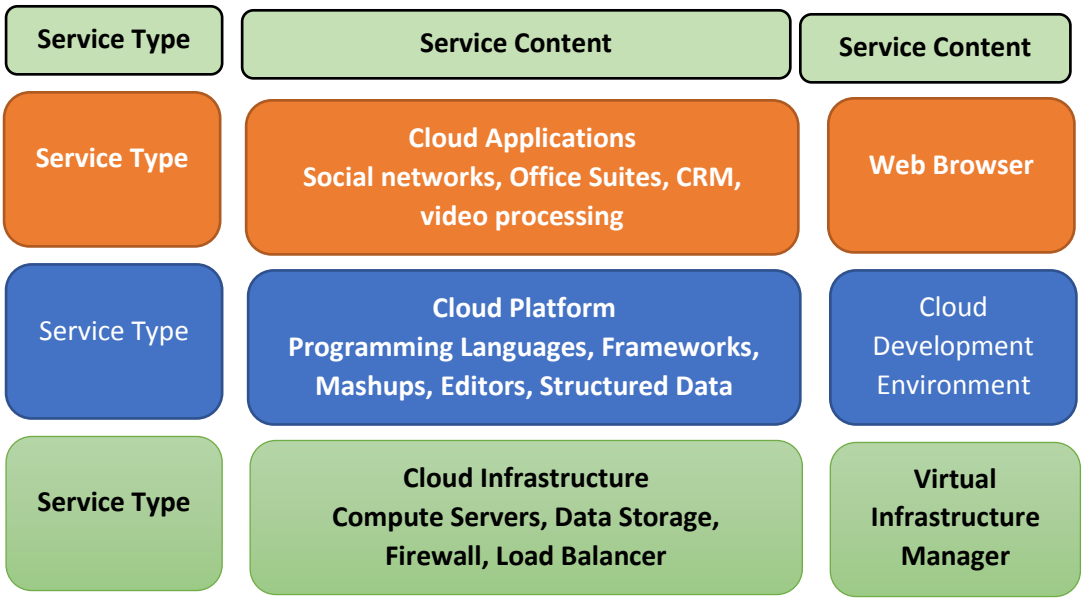

Figure 2.1: Cloud Service Models (Mell and Grance, 2009)

2.2.2 Infrastructure as a Service (IaaS):

Infrastructure as a service offers computing infrastructure solutions as a service to customers, mainly by providing virtual compute and storage capabilities. CSPs manage the physical resources, while customers run their software stack; manage the guest operating system and other allocated virtual resources. One of the benefits provided by IaaS is that customers have overall control over their data, and it gives them the ability to pay for what they use. Dropbox is an example of IaaS.

2.2.3 Software as a Service (SaaS)

Software as a service provides software applications that support users to address specific business functions, processes and other essential needs. In this service type, the CSPs manage the hosting environment and the software applications that are made available to customers. However, in some cases, customers are given the privilege to manage specific configurations within the supported software application.

2.2.4 Platform as a Service (PaaS)

A Platform as a Service is a software platform that can be used by customers to develop and host their software application or other information systems. Under PaaS, services are managed by the CSP while customers manage their software stack. An example of PaaS is Microsoft Azure.

2.3 Cloud Deployment Models

Cloud deployment models represent the specific category of the cloud environment. Cloud computing consists of four main deployment types:

2.3.1 Public Cloud

Infrastructure in public cloud is controlled by the CSP where resources are dynamically provided on a fine-grained, self-service basis over the internet and become accessible via a web application to the general public. The CSP usually manages the physical infrastructure, but some other specific functions could be outsourced to a third party. Public cloud is more suitable for businesses that require resiliency and elasticity of applications that many users can consume. This model is attractive because of its decreased capital overhead and operational cost. Amazon web services is an example of a public cloud.

2.3.2 Private Cloud

A private cloud involves a distinct, secure and more reliable deployment model that is owned and used by a particular specific company. It provides computing power to within a virtualized environment using an underlying pool of physical computing resources that are only accessible to a single company, thereby providing greater control and privacy. Businesses that have dynamic requirements, critical missions and uptime requirements are better suited to private cloud. In general, performance obstacles and security challenges can be evaded in a private cloud, but may also be prone to other vulnerabilities such as internal data theft. Example of private cloud deployment includes telecoms infrastructure and financial institutions.

2.3.3 Community Cloud

Community cloud allows business or organisations with common business functions, requirements or objectives to collaborate and establish their specific cloud infrastructure to realise some of the benefits of cloud computing. The community members generally share similar performance, privacy and security apprehensions. A community cloud can be hosted internally or externally, as well as internally managed or outsourced to a third-party provider. In particular, a community cloud is appropriate for businesses that work on a similar project or mission needing centralised capabilities for managing and implementing the project Examples of community cloud include banks and trading firms.

2.3.4 Hybrid Cloud

Hybrid cloud is a mixture of private, community or public cloud that are bound together to support higher availability, reliability and resiliency. Hybrid cloud permits a business to increase the capacity

or capability by assimilation or customization with another cloud service. In particular, resources are managed and provided either in-house or by external providers.

2.4 Security Issues in Cloud

Cloud computing continues to evolve and expand over time. New security challenges constantly emerge that create concerns and hamper the progress of wide-scale adoption (Pearson and Benameur, 2010a). The environment tends to be surrounded by complex issues that introduce significant risk to businesses (Bhadauria et al., 2011). As long as third-party services make up the cloud, the problem of security and privacy of customer data cannot be completely avoided. Apart from the security issues, cloud users are also apprehensive as to what security controls are available in the cloud to provide adequate protection as a result of relinquishing control of sensitive data and applications to a CSP (Zissis and Lekkas, 2012). Some of the pressing concerns to which a resolution is proposed in this thesis involve security risks to customer data and the insufficient monitoring resources for providing transparency. Other issues that aggravate the concerns are the insufficiency, or otherwise immaturity of CSPs to support prospective customers in ensuring the fulfilment of their security requirements. While these concerns are perspicuous, there other significant challenges in the cloud domain that have been cited in the literature and industry. This thesis summarises both industry and literature-cited security challenges that are relevant to the problem domain (Ryoo et al., 2014):

- **Loss of Governance:** The adoption and migration of enterprise or corporate data imply a partial surrender of control to the CSP, which results in losing some control over policies, procedures and monitoring of user data. This loss of control can generate other problems that affect policies, security or privacy procedures that are far within reach of the organisation.

- **Transparency:** Prospective cloud computing users opting to adopt cloud services usually raise concerns over lack of information on security controls, vulnerabilities, and threats and they do not have visibility into CSP activities that ensure policy and procedures are being enforced in operations. Organisations typically require details that may enable them to perform risk assessment and management on services offered. Furthermore, users have concern over compliance with privacy law and data governance that accommodates the application of policies and principles to protect customer data.

- **Trust Issues:** The complex internal setups of cloud computing sometimes makes it difficult for cloud users to acknowledge provider's trust owing to the user relinquishing direct control over many aspects of security and privacy to the provider. Also, as data is being stored and processed by a third party, which is confined outside the vicinity of an organisation that is being protected with security controls, it escalates the level of risk and instils fear to the cloud users.

- **Data Loss:** Public clouds store the data of multiple users on a shared environment where a loss of privileged access may bring a severe security concern to other cloud users. Accordingly, lack of proper information management such as the use of appropriate encryption algorithms, authentication and access privilege result in sensitive damages and unexpected leakages. Therefore, user data at rest, in transit or use, needs to be controlled and protected using cryptographic measures and standard communication protocols.

- **Ambiguous Accountability:** Accountability involves defining compliance to internal and external governance criteria, implementation of suitable actions such as contractual and legal requirements, substantiating such actions and accepting the responsibilities for failure to act appropriately. The lack of a clear definition of accountability and responsibility among CSPs and users may bring about the conceptual problem between them, and this may create a contractual inconsistency that may further induce anomaly or incidents.

2.5 Security Controls in Cloud

Security is essential but also a challenging aspect of cloud systems. It refers to a broad set of technical and operational safeguards deployed to protect data and applications and address the security challenges associated with cloud computing (Krutz and Vines, 2010, Ramgovind et al., 2010). The rationale behind the need for security protection is the fact that once users' sensitive data are migrated to the cloud, it resides in the CSPs infrastructure and depending on the cloud service, a user may have little or no control over the data. The loss of full control over security may create other privacy issues that could hinder business processes (Rittinghouse and Ransome, 2016).

In general, many types of security controls are deployed within a cloud architecture, and they can be listed according to the area of application (operational or technical) and categorized by functionality (preventive, detective corrective and deterrent) (Krutz and Vines, 2010). Operational controls deal with policies, procedures, and standards that provide guidelines for facilitating the security of customer data from both customer and provider sides. Technical controls, on the other hand, involve a set of technical measures or strategies necessary to prevent, detect, and counter threats to customer data and the cloud systems. In this context, cloud security controls can be classified according to:

2.5.1 Preventive Controls

Preventive controls aim to prevent security violations, malicious actions and enforce access control against customer's data. Example of cloud preventive controls include encryption, intrusion prevention systems (IPS) and firewalls

2.5.2 Detective Controls

These controls are put in place to help detect violations and malicious activities. They do not stop or mitigate malicious activities, but only identify and report attempts or occurrence. Examples include intrusion detection systems (IDS), security logs and audit trails.

2.5.3 Corrective Controls

Corrective controls attempt to reinstate, correct or restore a cloud system to normal process after a security violation has occurred. Examples include: repairing the operating system of a host cloud machine or restoring data from a recent backup.

2.5.4 Deterrent Controls

A CSP implements deterrent controls in an attempt to discourage attackers from attacking cloud systems. A cloud user could also employ a visible practice of sound information security management to deter potential attackers. Example of deterrent controls includes monitoring and logging.

2.6 Related Works

In this section, related works in the area of virtual machine monitoring, cloud compliance; software-agent and security audits as a transparency mechanism are presented. Other works that are not explicitly meant for addressing clouds security transparency but can be used for the purpose are also discussed. This includes a discussion of works in the domain of audit and assurance, best practices, cloud forensics, including security incident management. A review of literature in these areas allows the reader to understand the limitations of the current state of the art, gain an understanding of the cloud security transparency-related problems and form the basis for this research.

2.6.1 Audit and Assurance

One of the major concerns when moving data to a cloud environment is the loss of control over the data. In a typical non-cloud scenario, an organization knows where correctly data is stored (e.g. on which server and disks), but this is not the case in the cloud, due to information hidden by the CSP as well as the use of distributed file systems in the cloud. As a result, new mechanisms and approaches to assuring the auditability of data in the cloud have been proposed. A literature review is presented in this context to highlight the current state of the art in cloud auditing domain.

2.6.1.1 Data and Storage Integrity Audits in Cloud

One of the approaches to cloud audits is to assure the integrity of cloud-based storage service where data is stored in the cloud is downloaded and checked for completeness, thereby enabling transparency. Recent works performed in this area include:

Tian et al. (Tian et al., 2019) presented a cloud storage auditing technique that aims at addressing the challenges associated with determining CSP conformance to the legal expectations of users using data integrity auditing scheme. The approach proposes a public auditing scheme that encompasses identity-

privacy preservation, group dynamics and identity traceability, and batch notification. It adopts a Boneh-Lynn-Shacham (BLS) signature technique to generate homomorphic authenticators that preserve the identity privacy of users, and random masking that blinds data proof as a means for protecting data privacy.

Identity-based integrity auditing for cloud storage is presented by Shen et al. (Shen et al., 2018). The authors proposed a new scheme for remote data integrity auditing called identity-based shared data integrity auditing which encrypts shared sensitive information before sending it to the cloud and then generates signatures that are used to verify the integrity of the encrypted file. In the scheme, a sanitizer is used to sanitize data blocks corresponding to sensitive information of a sensitive file, a user then blinds the data blocks which correspond to the original sensitive information and generate the corresponding signature before being sent back to a sanitizer. The blinded data blocks are converted into a uniform format, including the confidential information.

Secure storage, verification and auditing (SecSVA) of data in the cloud is presented by Aujla et al. (Aujla et al., 2018). SecSVA aims to ensure secure third party auditing with integrity preservation in the cloud environment. It consists of several modules that include an attribute-based secure data duplication framework, and a secure Kerberos that is designed for secure auditing of data stored in the cloud in which different algorithms for key generation, encryption, and decryption are designed. The architecture of SecSVA supports data authentication, verification, auditing, integrity and confidentiality for cloud storage.

Similarly, Sookhak et al. (Sookhak et al., 2014) developed a remote data auditing method which uses an algebraic signature that allows clients to efficiently check data possession in cloud storage while incurring less computational overhead on the cloud side and client-side compared to homophobic cryptosystem. The work extended data auditing scheme by designing an efficient data structure that could support dynamic data update features with minimum computation overhead on client and cloud service sides. They implemented the scheme to prove its security and performance in comparison to other data auditing methods.

The fundamental principle of any data-centric audit requires the checks for the completeness and integrity of data stored in the cloud. The literature presented in this context provides promising mechanisms for ensuring security transparency through integrity audits. These approaches may be necessary for small datasets, but it is mostly infeasible and might be prohibitive due to downloading large datasets in terms of bandwidth cost and overhead performance; hence, very impractical. Also, the computation cost on the server-side for generating proofs could limit how a user can frequently verify the integrity of outsourced data. Also, the additional metadata that is required along with the original data stored in the cloud creates storage overhead on both the client and server sides, which, in turn, creates storage inefficiency.

2.6.1.2 Regulatory Compliance, Standards and Best Practices

Relevant standards and best practices have become prominent features in the realm of security transparency through evaluating security and privacy controls in cloud computing. Most of these frameworks are considered in general ICT, e.g. (27001, 2013, COBIT, 2019) describe security protection mechanisms including organizational and technical controls for preventing data breaches, ensuring integrity and privacy protection.

Cloud Controls Matrix is developed by CSA (Cloud Security Alliance, 2017a), which aims at producing best-practice and a solid foundation for security transparency. Its goal is to provide fundamental security principles that guide and supports cloud users in assessing the general security risk of a cloud service. It gives a detailed description of security principles that are based on established control frameworks, standards and regulations such as ISO 27001/27002, PCI-DSS among others

Another essential project by the CSA is the Consensus Assessments Initiative Questionnaire (CAIQ) (Cloud Security Alliance, 2017b). CAIQ is intended to assist cloud auditor and users in evaluating the security services of a CSP using a list of questions they might want to ask a CSP. CAIQ provides numerous advantages to the CSP such that it enables the provider to submit their response in a public domain for every potential customer to access.

Security, Trust & Assurance Registry (STAR) (Cloud Security Alliance, 2017c) is another initiative that provides a public database of CSPs that have completed assessment based on CCM and CAIQ. It comprises different levels of START certifications ranging from self-assessment, which is self-explanatory, certification and attestation which require an evaluation by a third-party, and continuous, which is a certification based on constant monitoring.

Similarly, some recent work on accountability in the cloud have emerged through projects such as A4CLOUD, whereby researchers are thriving to devise models that can help put in place a set of mechanisms that ensure CSPs are held accountable for breach to SLA or a security incident that can be traced back to a lax in their security. In the context of A4Cloud, the concept of transparency in the broader sense is considered as an attribute of Accountability (A4 Cloud, 2017).

The European Union Agency for Network and Information Security (ENISA) developed a framework that enables cloud customers to collect assurance information about the security protection of assets from CSPs. The framework provides a set of questions that potential cloud customers may wish to ask about a CSP. The questions are mostly based on industry standards such as the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO) standards (European Network and Information Security Agency, 2010).

All of the initiatives mentioned above are subject to an audit that aims to ensure security transparency and assure a certain level of compliance to established criteria. Audits are usually conducted to evaluate

compliance with one of these standards as part of a certification process. However, the intervals at which the audit is performed is generally quite long (yearly or longer). There is the potential that policy violations can remain undetected, and the frequent probing of violations is not considered. An important aspect that needs to be addressed is the period of uncertainty by enabling continuous assessment of cloud operations in respect to conformity to requirements. In addition, best-practice like the CSA STAR provide a pre-assessment metric that measures the transparency level of various CSPs before cloud services are adopted or provide a mechanism by which cloud users ask for and receive information about elements of transparency supported by a CSP. But it fails to acknowledge the tendency of CSPs to generate a false representation of their services without continuous verification.

2.7.2 Cloud Forensics

Cloud forensics deals with the process of performing a structured investigation by collecting and analysing digital information to reconstruct security events while also protecting the privacy rights of cotenants in a cloud infrastructure. Cloud forensics is an essential element of security transparency by enabling the identification, collection, preservation and analysis of data so that it can be effectively used to establish the integrity of data. New techniques and methodologies are being developed for cloud forensics.

Virtual Machine Introspection (VMI) is one of the techniques used for providing evidence in cloud forensics (Pape, 2017). VMI leverages the capabilities of a hypervisor to examine the virtual machine at runtime for intrusion detection activities (e.g. malware detection on introspected VM). Deshpande et al. (Deshpande et al., 2018) proposed a logging and replay system that analyses intrusions, which runs in a VM, performs logging in the host OS and replays the whole VM process for analysis and improving the transparency of VM runtime.

Borisaniya et al. (Borisaniya and Patel, 2019) argued that VM monitoring is a promising technique for activity detection at the hypervisor level. The authors proposed a VMI security framework that leverages derivation-based approach to monitor activities running inside a VM, which utilises the hardware-based system call tracing tool to extract system call traces of VM processes. It uses a derivation-based approach to monitor activities running inside the VM from outside by extracting system call traces of each process and detect any potential malicious activity.

In Lauren et al. (Laurén and Leppänen, 2018), a web-based monitoring system for VM called Nitro Web is presented. Nitro Web is capable real-time of data collection, detection and visualisation of call activities taking place within a VM, which is built on top of Nitro, a python-based VMI framework for analysing VM state. The authors maintained that the Nitro Web provides a transparency VM monitoring capabilities because it does not require involvement or cooperation from the guest OS being monitored.

A Cloning and Injection based VM Inspection in Cloud (CIVIC) is proposed by (Suneja et al., 2017). CIVIC is a mechanism that enables inspection of production VMs by creating a replica of the VMs

runtime state in a spate isolated sandbox environment. It then uses a runtime code inject to introduce userspace-level functionality for over the replicated VM state to avoid guest modification. CIVIC enables VM introspection based monitoring and inspection solutions.

Jia et (Jia et al., 2017) proposed an architecture (T-MVI) that prevents the malicious access to VM data and subversion of regular VM routine. The technique guarantees VM integrity by monitoring the contents of a virtual machine in real-time from the hypervisor level. Their architecture examines and eliminates the risks of privacy leakage and security bypass through isolating the core code for virtual machines to an isolated environment within the hardware component. The authors maintained that the proposed architecture could prevent attackers from hijacking the data emanating from VM or falsify information to gain illegitimate access to the computing node. However, the work failed to demonstrate how captured information about VM is communicated or analysed for identifying security lapses and vulnerabilities to the VM.

In Deshpande (Deshpande and Ainapure, 2016), the authors contend that virtual machine introspection serves as a right solution for monitoring malicious activities in VMs such as taking control of host privileges through software loopholes or attacks on virtual machines in the same cloud platform. To mitigate the problem, they proposed an intelligent real-time virtualisation monitoring system that continuously checks the status of guest VMs in both static and dynamic modes to identify and prevent cloud resources from attacks. The approach aims to achieve reasonable efficiency and security by ensuring that VM is protected from various forms of attacks and to add intelligence to VM introspection by embedding a pattern recognition algorithm for identifying threats. The authors used a system call tracing tool which monitors the status of virtual machines. However, the work is mainly built on static threat pattern recognition that is not dynamic enough to identify emerging threats

Tovarnak et al. (Tovarňák et al., 2014) identified the lack of multi-tenant monitoring support and limited access to provider controlled monitoring information prohibits cloud customer from determining the status of resources of their interests adequately. To address this problem, they proposed a distributed event-driven monitoring model for enabling multiple simultaneous consumers a real-time collection and analysis of monitoring data related to the behaviour and state of many distributed entities. The contribution emphasises the use of behaviour monitoring that includes the collection and analysis of data related to the actions and changes to the state of the resources monitored to detect behaviour deviations and their patterns.

The most important aspect of cloud forensics as proposed by the literature, as mentioned above involves the heterogeneity and availability of evidence, and access to evidence sources, which are vital to ensuring security transparency. However, the application of VMI for cloud forensics faces many challenges. For example, the legal authority and time synchronisation due to the distributed nature of cloud services, as well as the preservation of evidence integrity, chain of custody and availability of

sufficient storage capacity are some of the significant drawbacks in the proposed approaches. Other challenges include the protection of privacy rights in a multitenant environment when investigators collect evidence. For instance, if a VM that runs in a cloud server becomes the object of interest in a forensic investigation, the entire server may be seized by the law enforcement, and this may result in co-located VMs owned by other tenants to be affected. In particular, the CSP may be unwilling to provide an investigator with the required access to physical machines, and in some cases, such as where multiple jurisdictions are involved, the CSP may not be obligated to do so. Furthermore, another major problem is dynamicity, i.e. cloud forensics does not mainly focus on the areas of security that are of significant importance to the cloud customer. The failure to appropriately harbour customer expectations amounts to ineffectiveness to dispense transparency unless otherwise done differently.

2.7.3 Software Agent and SLA Monitoring

Ouedraogo *et al.* in (Ouedraogo et al., 2015b) proposed one of the first solutions for promoting security transparency in the cloud realm. Their contribution, which is event-driven, allows both CSU and CSP to make specifications to represent patterns of events, whose occurrence can be an evidence of a security anomaly or breach or merely a sign of nefarious use of the cloud infrastructure by some of its users. Casola *et al.* in (Casola et al., 2015) presented a monitoring architecture that integrates different security-related monitoring tools to provide continuous monitoring capabilities for SLA security parameters. The monitoring architecture put forward by the authors is built on and integrated with monitoring components belonging to SPECS framework, which also aims at designing and implementing a management framework of the SLA lifecycle.

Casola *et al.* in (Casola et al., 2014) also discussed a preliminary design and implementation of a security solution for PaaS based on SLA approach to address the issues related to the management of security requirements in the cloud. The work adopts a dedicated cloudware platform that is deployed over infrastructure resources. The platform supports end-users and CSPs to specify their security requirements using SLAs, evaluate security features offered by remote cloud security brokers, management of SLA lifecycle as well as the development and deployment of security services.

Pauley (Pauley, 2010) developed an assessment scorecard that assesses the transparency worthiness of CSPs from three dimensions, namely: security, privacy, auditability and service level agreements. In Pauley's contribution, a pre-assessment can be performed on CSPs based on three factors relating to the CSP and their business entity. The scorecard consists of a pre-assessment phase that is used to generate and assign values to a CSP, based on which threshold values are compared to determine if the CSP is eligible for another assessment at post-assessment phase. At the post-assessment stage, the transparency worthiness of a CSP is compared against a set of questions that have been formulated based on the four dimensions. The approach also considers several factors relating to a CSP to support organisations to perform the assessment. Such factors include CSPs', years of business, published

security or privacy breaches, published data loss, profitable or public, similar customers, membership to standards etc. This approach serves as a guideline for organisations to evaluate CSPs transparency. However, it is quite complicated and does not appear to be useful for an organisation with a broad set of requirements.

Garg et al. (Garg et al., 2013) proposed a framework that enables cloud users to compare different cloud offerings based on specific user requirements using analytical hierarchy process (AHP) approach (Vaidya and Kumar, 2006). This particular framework utilizes specific cloud service measurement indexes such as accountability, agility, assurance, cost, performance, security and privacy, and stability.

In addition, CloudHarmony (Leitner and Cito, 2016) developed an online cloud measurement tool that enables customers to evaluate the performance of CSPs. The platform consists of four major components: CloudSquare, CloudScores, CloudReports, and CloudMatch. Cloud customers can use CloudSquare to search and compare services provided by CSPs based on attributes such as price, performance, and geographical location. CloudScores provides customers with access to benchmarking metrics that evaluate the performance of cloud services based on memory, CPU, and network, while CloudReports provides analytical reports of CSPs performance. CloudMatch, on the other hand, allows customers to perform tests such as the speed of uploading and downloading large files and network latency across different geographical locations. However, this approach mainly focuses on the evaluation of CSPs based on certain variables but does not consider CSP security and compliance.

In addition, Li et al. (Li et al., 2010) developed a framework that aims at assisting potential cloud customers in evaluating the performance and comparing the cost of CSSPs, based on a set of metrics including storage, memory and network. The framework consists of a tool called CloudCmp that is designed to perform this comparison. The tool is used to perform a study on the major cloud providers in the market. However, similar to CloudHarmony, the evaluation focused on specific attributes that are not security oriented

The works, as mentioned earlier, are associated with several limitations. For example, one problem deals with dynamicity, i.e. it does not mainly focus on the areas of security that are of significant importance to the cloud customer. The failure to appropriately harbour customer expectations amounts to ineffectiveness to dispense transparency unless otherwise done differently. Other transparency initiatives by the research community either serve to provide a pre-assessment metric that measures the transparency level of various CSPs before cloud services are adopted or provide a mechanism by which cloud users ask for and receive information about elements of transparency supported by a CSP. The need for continuous visibility and transparent probing of activities based on evidence is not considered. The works also failed to acknowledge the tendency of CSPs to generate a false representation of their services without continuous verification. Another limitation deals with the unfeasibility of attaining absolute transparency on all the clauses within an SLA, which could be ascribed to the security or legal

constraints that may restrain CSPs from making certain disclosures, as well as the enormity or otherwise practicality of all areas of cloud security that ought to be covered.

2.7.4 Industry Practices and Systems

When exploring the associated processes, methods and initiatives for enabling security transparency, it is vital to consider existing industry practices. Various vendors in the cloud industry have developed systems and associated processes for distributed data collection for monitoring purposes in cloud infrastructure, such as the renowned Nagios (Nagios, 2017), which supports distributed data collection and analysis. Most of these systems are mainly Security Information and Event Management (SIEM) systems, which serve as the means for detecting security events and collecting information from various sources. Therefore, in the following, the characteristics of some of the currently powerful commercial SIEM solutions for both cloud monitoring and data centre is presented. The list is based on a review by Solutions Review (Solutions Review, 2017), which evaluates the strengths and weaknesses of these systems.

IBM developed QRadar SIEM (IBM, 2017) that is available as a hardware virtual appliance and software packages based on the customer's event velocity. It includes several components such as network insight, user analytics that addresses insider threat use cases, and an advisor that provides automated root cause research for identified threats. McAfee SIEM (MacAfee SIEM, 2017) is developed to deliver application monitoring and threat intelligence capabilities. It provides real-time status and understanding of threat data, as well as a view of the systems, risks, and activities of cloud systems.

Also, Amazon CloudWatch (CloudWatch, 2019) allows the monitoring of AWS resources and applications to run on AWS in real-time to collect and track metrics and automatically displays the metrics being used by AWS service user, including the capability to manage logs and set incident alarms.

LogRhythm (LogRythm Inc., 2017) combines log management, event management, file integrity monitoring and machine analytics with host and network forensics in an integrated security intelligence platform. It helps in the collection of security event log data throughout cloud systems, including network security controls, user applications and operating systems, including to analyse data to identify possible signs of malicious activity and to help recover from successful attacks.

Alert Logic (Alert Logic, 2019) provides Security-as-a-Service for on-premises, cloud and hybrid infrastructures to deliver deep security insight and continuous protection. Depending on the cloud service provision model, it considers cloud security to be a shared responsibility between the CSP and the customer concerning information security.

Logentries (Logentries Inc., 2019) is another product that provides real-time log management and analytics services. It is delivered as a SaaS and enables secure collection and analysis of log files while preventing leakage of unencrypted sensitive data. Logentries includes alerts to identify security threats and investigation of malicious activities. Also, it enables the management of vast amount of data, visualisation and automatic analysis and reporting security incident.

Rackspace Monitoring API (Rackspace, 2019) currently supports monitoring for external services and allows customers to query the Rackspace cloud management system (CMS) for performance metrics on the CSP infrastructure. Generally, Rackspace monitoring API enables customers to simultaneously monitor the performance of different resources from multiple data centres and enables the collection of a variety of data that can be used for measuring critical data.

Salesforce ReST API (Salesforce, 2019) provides a ReST API for event monitoring data that contains useful for assessing usage trends and user behaviour. It can be applied to integrate log data within back-end storage and data marts to correlate data from multiple and disparate cloud systems. It also includes an audit trail generator for costuming actions done by service administrators.

EventTracker (Netsuron EventTracker, 2019) is another SIEM solution that integrates prediction, prevention, detection and response service offerings primarily to midsised commercial enterprises and government organisations with SIEM compliance reporting requirements. EventTracker also provides support for file integrity monitoring, as well as add-ons for vulnerability and configuration assessment.

Many of the above-stated industry systems make use of logging data generated in the cloud infrastructure, and they have numerous strengths and weaknesses. However, such systems are designed to capture log data from a specific area of the cloud infrastructure (such as network or database activities), and the extent to which logging information is captured from the cloud environment is dependent on the focus of the tool. They do not provide vital information regarding other layers and heterogeneous sources of the cloud stack

2.8 Chapter Summary

In this chapter, a brief discussion of the primary service model and deployment models of cloud computing have been presented to establish a common understanding of the research domain. A particular focus is on current security issues considered as problematic; mostly over aspects of cloud security transparency, privacy and governance concerns. Additionally, the chapter presented some elements of security controls in cloud computing. Importantly, the chapter elaborates on how the existing approaches that influence security transparency in cloud. A particular focus has been placed on the relevant literature on cloud audit, cloud forensics, and industrial systems, including evidence collection and assessment since these two properties are essential aspects of the proposed framework. Contemporary works from these domains are considered because one of the significant problems in cloud security transparency is the lack of evidence collection and analysis regarding the controls

implemented by CSPs. In this research, it is argued that customer trust can be increased if CSPs act and implement appropriate data protection machinists according to customer expectations by providing evidence-based assessment capabilities.

CHAPTER THREE

Research Methodology

3.1 Introduction

A research methodology is an essential tool for identifying existing problems which need to be investigated and reach the objectives set out for particular research (Kothari, 2004). It can be seen as a method for collecting meaningful data and performing a systematic analysis to get accurate and realistic results. Research methodology clarifies the study's aims and identifies the elements that are pertinent to the research needs (Neuman, 2013). Mackenzie and Knipe (Mackenzie and Knipe, 2006) noted that research methodology highlights how techniques and procedures in the research design can be used, distinguishes between methods and results, and also crucial for achieving and clarifying key research aims. Generally, the purpose of research methodology can be described as giving a clear idea of the methods or processes that should be used to address the research problems. Therefore, research methodology is an essential element which clarifies all the steps needed to achieve the research objectives in this thesis.

This chapter presents an outline of the techniques and theories applied in developing the proposed framework, including the research approach employed to validate the Cloud Security Transparency Framework (CSTF). Specifically, a combination of three important steps is used, consisting of a literature review, framework development, and evaluation process.

3.2 Methodology for Framework Development

The framework development process is mainly guided by a combination of theories, industry standards and methodologies. Figure 3.1 provides an insight into the steps used in the methodology for framework development.

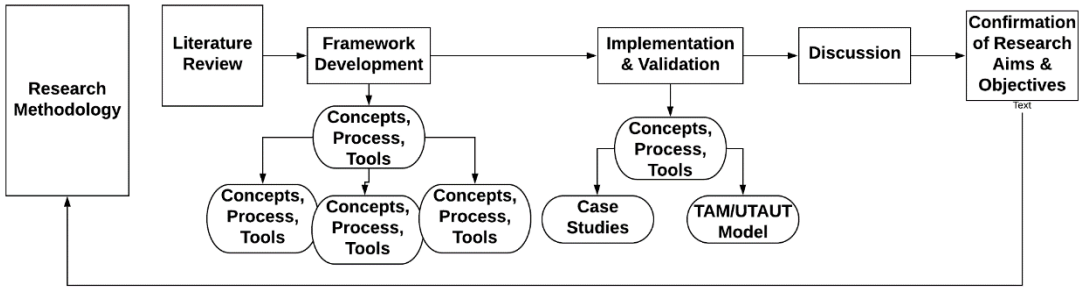

Figure 3.1: Methodology for Framework Development

3.2.1 Step 1: Literature Review

The first step involves the application of a methodology for reviewing existing literature. It is mainly carried out to identify, analyse and summarise the present state-of-the-art literature concerning the methods and approaches for enabling cloud security transparency. Evidence from the literature is

pointed out to outline various techniques that are adopted for developing CSTF, addressing research questions, aims and objectives.

3.2.2 Step 2: Framework Development

The second step deals with the development of CSTF, which incorporates many concepts, a unified process and tool support for performing an audit. The concepts constitute and provide the high-level foundation for understanding security transparency from conceptual, organizational and technical perspectives. The process describes different phases of activities which can be followed by any organisation to achieve security transparency, and lastly, security transparency and audit tool is specifically designed to support organisations utilize security audit as a means for achieving security transparency

In developing the framework, several techniques, theories and standards are employed for ensuring that it is developed and implemented according to generally accepted principles. In particular, sections from renowned industry standards, guidelines, frameworks and models were applied across different activities within the process by looking at specific features within the standards and where they can be applied in the process. The following section provides an insight into the many techniques and standards used:

3.2.2.1 Secure Tropos

The proposed framework needed to be developed based on standard methodology, and for that reason, Secure Tropos was considered (Mouratidis and Giorgini, 2007). Secure Tropos is a novel agent-oriented software development methodology that covers development process from initial requirement analysis to detailed design, which allows for greater understanding of the operational environment of a software system (Bresciani et al., 2004). Therefore, the research follows a set of concepts, such as actors, constraints, and goals based on Secure Tropos (Mouratidis and Giorgini, 2007). Secure Tropos uses the concepts of actors, goals and social dependencies to define and view a multi-agent system and its social dependencies as a set of actors from within organizational settings (Giorgini et al., 2007). The research extends secure Tropos by using new concepts such as evidence, risk, and audit in an attempt to develop the proposed framework. The reason for choosing Secure Tropos is that it is well suited for modelling security requirements and provides in-depth analysis of security issues from organization and its social setting. The concepts of Secure Tropos and those proposed in our approach are integrated to enable the identification of goals, assets, and assessing CSP evidence.

3.2.2.2 Ontology and Semantic Web Language

Ontology is a formal language that allows the explicit specification and conceptualization of ideas that represent the abstract model of a phenomenon (Maedche and Staab, 2001). It enables the construction of knowledge and provides the advantage of knowledge representation in organized metadata of complex information resources (McGuinness and Van Harmelen, 2004). The metadata provides

semantic information about resources which are encoded as instances. The proposed framework comprises various concepts that represent abstract ideas in the domain knowledge of transparency. Ontology is used to provide an explicit knowledge-based understanding of the attributes, relationships, restrictions and rules between the concepts.

3.2.2.3 Industry Standards

Renowned industry standards, guidelines, frameworks, methodologies and models were followed in developing the framework, some of which include:

- *CSA CCM:* is used because it provides a set of controls that provide fundamental security principles to help cloud computing customers and vendors achieve security relating to information asset protection in the cloud industry (Cloud Security Alliance, 2017a). The CCM was adopted to specify essential security requirements for asset protection that must be met by the CSP, and form the basis of a security audit.
- *CSA CAIQ:* provides a template questionnaire containing a set of questions that can be used by auditors to assess the security capabilities of a CSP (Cloud Security Alliance, 2017b). CAIQ is considered for creating security audit checklist that for obtaining assertions and evidence from CSPs.
- *CIS CSC:* is designed to help organisations safeguard their assets. It consists of critical and actionable controls that are designed to defend organisations against known attacks, achieves higher overall cybersecurity defence, and implement a coherent security program.
- ENISA Cloud Controls: provides a guide to assess organisations' security risks that are CSP-oriented and focuses on control measures that protect cloud computing systems against operational risks (ENISA, 2016).
- ISAE 3402 Standards: provide guidelines for the conduct and performance of security audit according to established criteria and procedure (ISAE500). This standard is employed in establishing audit criteria for assessing CSP evidence.

3.2.3 Step 3 Research Validation

An empirical research method is selected for implementing and validating the contributions of this research. According to Euneson et al. (Runeson and Höst, 2009), empirical studies are increasingly becoming popular in information systems research because it has proven to be an effective research method to collect relevant data for investigating a specific problem in information systems. Therefore, a case-study approach was employed to validate the contributions of this research. The case study approach is widely used in research domain because it is useful for an explanatory research project, and serves as the basis for the development of well-structured research findings (Straub et al., 2004). The rationale behind employing a case-study is to obtain meaningful feedback regarding the validity of

CSTF as well as stakeholders views on the usefulness of STAT and then analyse the feedback to determine the acceptability and validity of the proposed framework.

3.2.3.1 Technology Acceptance Model

In formulating and evaluating the questionnaire used in collecting stakeholders' feedback, we use the renowned Technology Acceptance Model (TAM) (Davis, 1989) and the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003). TAM deals with the prediction of the adaptability of a newly developed information system by users within an environment, to determine its acceptability to a context and the modifications that need to be made to make it acceptable to all users. The authors maintained that the acceptability of any information system is determined by two major factors: perceived usefulness and perceived ease of use. Perceived usefulness entails the degree to which a person believes the use of a system will improve his performance (Davis, 1989). Perceived ease of use refers to the degree to which an individual believes that the use of a system will improve performance. On the other hand, UTAUT proposed four constructs, namely: performance expectancy, social influence, effort expectancy, and facilitating conditions that are direct determinants of usage of intention and behaviour (Karahanna and Straub, 1999). Therefore, TAM and UTAUT were selected as they appear to have some relationship in their constructs for in evaluating feedbacks.

3.3 Research Approach

A research approach is a systematic and orderly application of numerous steps for the collection, analysis and interpretation of data to draw meaningful insights and conclusions (Amaratunga et al., 2002). Orlikowski and Baroudi (Orlikowski and Baroudi, 1991) state that it is imperative to understand the aims of research to clearly determine and choose a suitable technique to achieve the research's purpose. The authors further emphasised that when selecting a research approach, two factors need to be considered: the characteristics of the topic and the time to conduct the research. There are many types of research approaches such as inductive, deductive, descriptive, explanatory and experimental. Many of such different methods form the main pillars used in this study to identify, select and develop a suitable research design and technique for data collection and analysis. Research approaches can usually be categorised according to qualitative, quantitative or mixed methods. For each methodology, the primary methods and the various steps needed for the application of each method is provided

3.3.1 Qualitative Research

Qualitative research is associated with the social constructivist paradigm that prioritises constructed nature of reality, it is investigative and mainly used to discover the general perception of a particular group or audience regarding an issue (Kumar and Phrommathed, 2005). Qualitative research focuses more on recording and analysis to uncover the deeper meaning and significance of human experiences, which assists in understanding a phenomenon. Traditionally, qualitative research uses non-numerical data such as discussions, explanations, and conversations which makes qualitative data-rich with strong

potential for revealing complex phenomenon by focusing on problems in their social environments (Creswell and Creswell, 2017). A qualitative approach is used when secondary data are insufficient to achieve depth in research (Bryman, 2006). The interview is the most commonly used technique for data collection, and it can be undertaken using structured or unstructured questions, as well as a combination of both. Interviews can normally take place through face-to-face interaction or electronic platforms such as telephone or video conferencing. Figure 3.2 shows the main methods and steps involved in the application of qualitative research method.

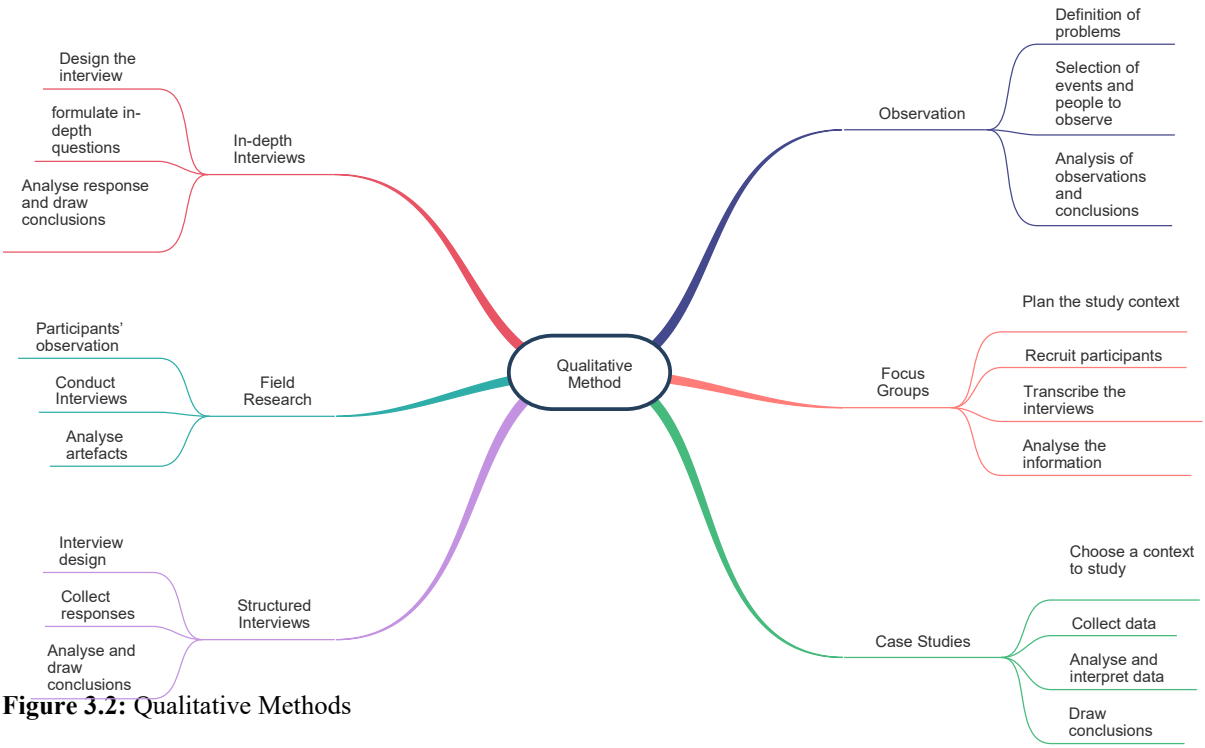

Figure 3.2: Qualitative Methods

3.3.2 Quantitative Research

The quantitative approach is associated with the interpretation of numeric data such as ratio, percentages or intervals, and using items of analysis such as diagrams or graphs for interpreting and visualising results (Bryman, 2006). In other terms, a quantitative approach is an empirical paradigm, which usually involves collecting and converting data into numerical form so that statistical analysis can be performed to conclude (Mugenda, 2003). The quantitative approach is predominantly used to quantify and interpret numerical data by surveying a target audience. An example of the methods used for collecting quantitative data is a questionnaire that contains a set of relevant questions for which answers are provided. Statistical techniques analyse the data gathered from the questionnaire and the results are generalised to the population (Burns and Bursn, 2000). Figure 3.3 shows the various steps involved in the application of a quantitative method.

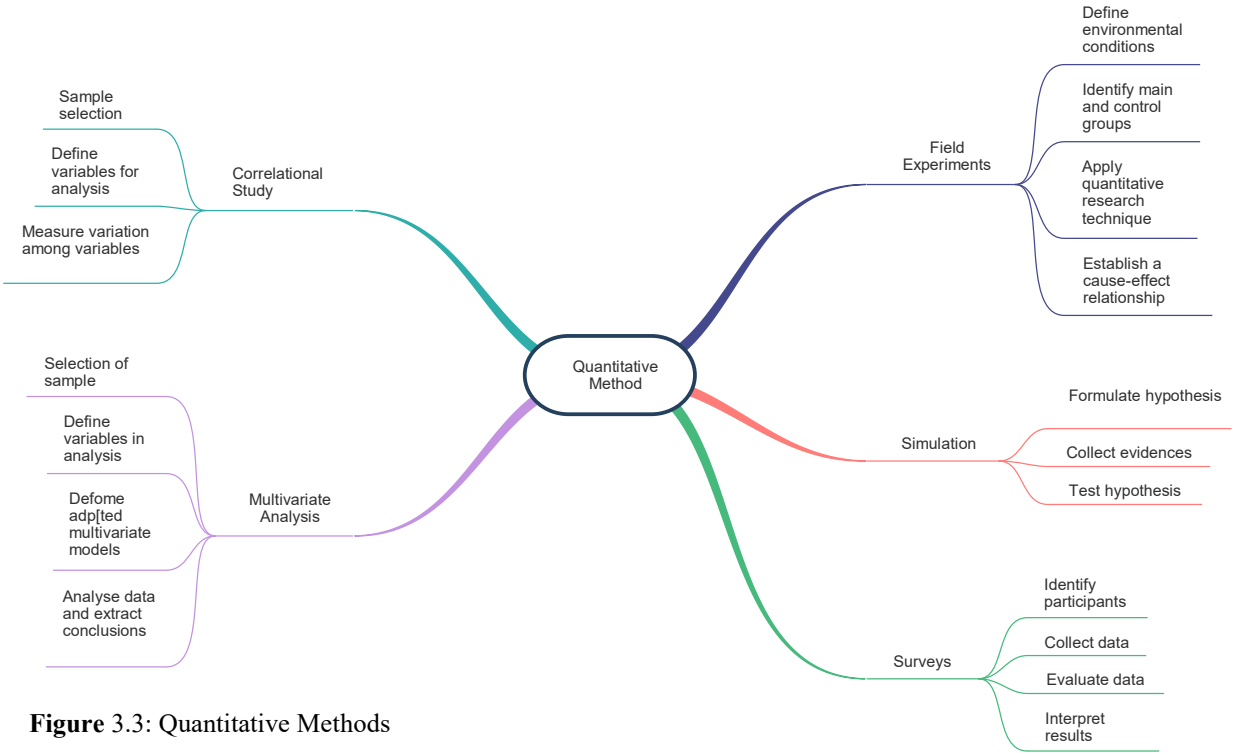

Figure 3.3: Quantitative Methods

3.3.3 Mixed Methods

Mixed methods consist of a combination of qualitative and quantitative approaches, especially in the aspect of data gathering, analysis, and interpretation (Creswell et al., 2003). A mixed-method provides more forms and options for approaches to consider. A vital factor to consider in any process is the reliability, which involves dependability, consistency, replicability of results (Amaratunga et al., 2002). A mixed-method ensures and improves the reliability of any research, and can be achieved through different procedures such as interviews and questionnaires. In addition, using a mixed-method, different type of data are collected from multiple sources, which add value and enhance the reliability of data and findings.

3.4 Research Method used for this Research

After the identification of the various and most commonly used research approaches, the next step is to establish a suitable research method that could be applied for this research. Based on the nature of this work, which involves the development, implementation and validation of CSTF, considering the research studies included, and the corresponding research questions whose aim is to contribute to the research goal, a qualitative research method was selected to guide the conduct of the research work. The rationale for using a qualitative research approach for this thesis include: qualitative study enables the understanding of a studied context by communicating with participants and capturing their experiences; it also allows the documentation of findings in more detailed and variable contents than in quantitative approach, and the study context materials can be evaluated with greater detail. Also, qualitative research allows the researcher to understand and present the context as it is seen and experienced by the stakeholders without predetermining those standpoints.

Additionally, for ensuring that logical research results are obtained, various research strategies that are associated with qualitative research method were applied. Case studies have been considered to guide the implementation, validity and usability of STAT. In particular, two case studies are used to evaluate the practical application in a real-world environment.

3.5 Research Design

A research design is described as a blueprint that provides a clear picture of the research structure, including the methods used for data collection, research questions and sources of data used in the conduct of the research (Denzin and Lincoln, 1994). Research design enables a researcher to outline all the tools needed for the research, such as selecting a suitable research methodology (Lewis, 2015). In other terms, research design focuses on the type of study to be conducted to reach specific outcomes and another way to see it is an action plan that provides a sequence of tasks or activities for getting from the research questions to results or conclusions (Maxwell, 2012).

Figure 3.4 provides an overview of the research design process followed in this work, which consists of five crucial stages. The first stage deals with review and analysis of existing literature within the problem domain to establish the knowledge gap. The second stage focuses on the development of CSTF for addressing purported research problems. The methods for the implementation and validation of the proposed CSTF are developed in the third stage, whereas the analysis and interpretation of data are performed in the fourth step. The last step deals with concluding the limitations of the study and future research work.

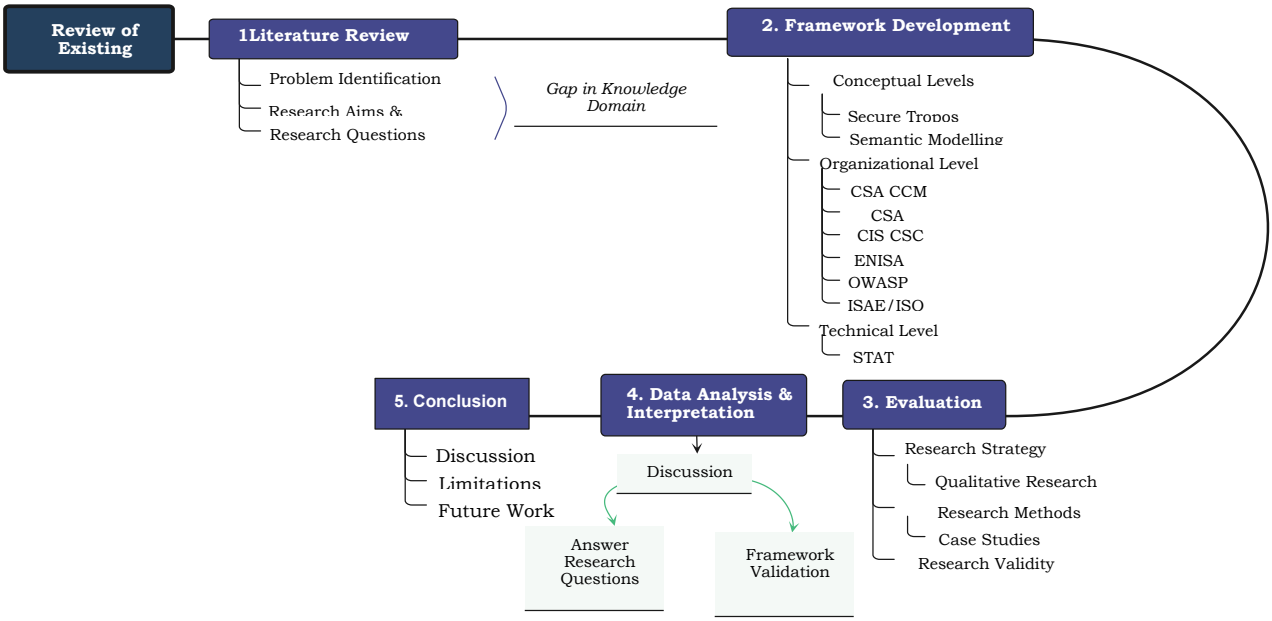

Figure 3.4: Research Design

3.6 Research Strategy

According to Berg (L BERG, 2001), research strategy is a step-by-step plan of actions that provides a researcher with the direction to conduct systematic research, using suitable methods to validate the study and to produce quality results and detailed findings. Oates (Oates, 2005) also stated that a research strategy enables a researcher to establish why a particular research method befits the research context and how selected methods address the research questions. Denzin (Denzin and Lincoln, 1994) further emphasised that research strategy deals with the improvement of artefacts and learning through making and invention or enhancements. Research strategy entails different components as research methodology, research design, and method of data collection, analysis and validation.

The choice of a research strategy is subjective and depends on the nature of the research problem. Various authors have presented different research strategies that can be applied to different contexts. Mills (Mills, 2000) has stressed that there are four fundamental types of research strategies that can be used: a case study, laboratory experiment, action research, and survey. However, when a new technology is introduced in an organisation, action research is usually conducted to explore and explain the socio-technical effects of the technology on users and operations. As a strategy, action research has been widely used in information system research because it aims to contribute both the practical concerns of people and to the goals of socio-technical paradigm. Thus, the author of this research has chosen action research using case studies.

3.7 Action Research

Action research is a term for several research practices applied in real-world situations to solve real-life problems by bringing together research and action, theory and practice, local knowledge and participation of people in research (Costa et al., 1991). A researcher in action research resides and interacts with a group of audience, participants or people for an extended period and engages them in an intensive and interactive learning process, which gives both the researcher and the participants a broad dimension of insights into various issues (Kemmis and McTaggart, 2005).

In evaluating the CSTF, a Participatory Action Research (PAR) has been adopted because action research emphasises on the collaborative participation of stakeholders within a case study context. Also, action research improves current situations being researched by direct implementation of research findings through the involvement of various stakeholders (Argyris and Schön, 1997). Further, action research allows a researcher to gather data using different methods such as case study, brainstorming, questionnaire, etc. Therefore, a case study was used, including the utilisation of a survey as a means for collecting data.

3.8 Case Studies

Eisenhardt (Eisenhardt, 1989) defined a case study as an empirical enquiry that attempts to investigate a contemporary phenomenon within a real-life environment mainly when the borderline between a

given phenomenon and context are not evident. A case study is often considered as a method that can investigate a contemporary phenomenon when there is a lack of knowledge and background is not clearly defined. Zainal (Zainal, 2007) stated that there are three main reasons to consider a case study research in the field of information systems: case study enables a researcher to study information systems in its natural setting and also enables the researcher to generate findings from practices; it also allows a researcher to explore questions to gain more explicit information

Therefore, the researcher established the importance of conducting the research validation for this work based on case study contexts that represent a real-world environment. The case study method is adopted because it enables the study complex research phenomenon and allows researchers to explore the research context in detail and draw a conclusion from the findings (Benbasat et al., 1987). The researcher has adopted two different case studies to demonstrate the validity of CSTF and STAT. The adoption of two case studies enables the researcher to study and compare the findings between different study contexts and thus allows the exploration of validity and usefulness of CSTF and STAT, which in turn enable the researcher to establish conclusions.

3.8.1 Case Study Selection

In terms of selecting the case studies, two criteria were set: the first criterion is for implementing the process for security transparency. For this aspect, only an organisation that newly adopted cloud services will be considered. The second criterion set outs to achieve the security transparency tool, which only considers an organisation that has already migrated to the cloud. Based on these considerations, contact introduced the researcher to two different organisations that fulfilled these criteria. The selected companies were:

- **Case Study 1:** considers a London based property management firm with six operational offices across multiple locations, five functional departments and a considerable workforce of more than 100 employees. The company also has more than 2,000 properties under its management. It uses an enterprise content management (ECM) system to provide fundamental capabilities that allow users to create seamlessly, edit, review, categorize, index, and publish contents on its website. The company decided to migrate a component of ECM called document management solution (DMS) to the cloud, and the implementation of CSTF is applied to this case study.
- **Case Study 2:** is based on a healthcare patient relationship manager (PRM) system that is owned by a borough in London. The system gives the swift public access to urgent care, treatment and advice for less critical medical problems, as well as providing clinical expertise, nurses and paramedics with integrated access to patients' health information and assessment tool. The system also provides doctors with access to relevant aspects of patients' medical and care information. The Borough has recently migrated some components of the PRM to the

cloud, and due to the nature and sensitivity of personal data of patients involved, it is concerned about the CSP's transparency in handling the system and ensuring the privacy of personal information. STAT was used in this study context for helping the borough achieve security transparency

3.9 Data Collection Methods

The collection of data from the case study is a necessary process and one of the most effective methods to uncover all relevant details relevant to the research (Cassell and Symon, 2004). Data collection and analysis significantly contribute to supporting the research idea. Polkinghorne (Polkinghorne, 2005) highlighted that three protocols need to be followed such as an overview of the case study context; field procedures, such as access arrangements to information sources, and case study questions that the researcher considers when collecting data. Polkinghorne (Polkinghorne, 2005) further stated that there are different sources to collect data in case study contexts such as interview, documentation, and observation, while Yin (Yin, 2009) noted that six main methods can be used to collect data including documentation, informal meetings and workshops, focus group interviews, direct observation, participant observation and physical artefacts. Various data collection techniques are used in the course of implementation in the case study contexts. Also, informal and formal data gathering techniques were employed such as an interview. Table 3.1 provides a hint of the data-gathering methods used during the implementation process.

Table 3.1: Data Sources

Data Source	In the course of	Used for
Documentation	Initial steps for framework and tool implementation	Obtaining preliminary and background information about the case studies in terms of understanding the scope of processes and portfolio.
Informal meetings and workshops	Throughout the implementation process	To provide an introduction of the process and tool to relevant stakeholders, and to provide them with directions throughout the implementation process.
Interview and questionnaire	Throughout the implementation process	To support the evaluation of the implementation process of CSTF and tool based on a combination of subjective and objective questions.
Observation	Throughout the implementation process	To closely monitor and observe how the stakeholders implemented the framework and the tool.

3.9.1 Context of the Study and Participants

The context of the survey involves two companies. The first company implemented CSTF, while the second company implemented STAT. Within these two companies, the questionnaire was distributed to various information systems roles: system administrator, security auditor, security analysts, IT manager, and top management. All the respondents have an average of 3 years of working experience, which was an added advantage for the researcher to ensure that respondents are knowledgeable enough to answer the questions and provide obtaining professional feedback.

3.10 Summary

This chapter presented a detailed narration of the research methodology adopted in the development and evaluation of the proposed framework. It outlined three important steps that have been taken, including a systematic literature review process, framework development, evaluation, discussion, and confirmation of research aims and objectives. It also presented the types of research approaches that exist and the chosen approach for this research. A research design is presented to provide an overview of the research structure, including methods used for data collection.

CHAPTER FOUR

Contextualisation of Cloud Security Transparency

4.1 Introduction

The previous chapters have presented a background discussion on cloud computing and some important facets that underpin cloud security transparency. This chapter dwelled on elaborating the notion of transparency from broad-spectrum and narrowed into the specific perspective of cloud service. It also introduces a conceptual definition of transparency based on a critical analysis of the attributes that constitute transparent operations. The perspective followed particularly enables the review and extraction of the attributes of transparency by considering similar works in the areas of social sciences, accounting, economics, and of course, cloud security transparency. The chapter has discovered that the common notion that binds most contributions together is the belief that information must be disclosed to attain transparency. Information disclosure, however, is insufficient to methodically constitute transparency in the cloud domain as there are other essential auxiliary properties and processes required for a flourishing efficacious *modus operandi*.

4.2 Transparency Basics

Transparency in the past few years has received considerable attention across several domains as a result of the surge to access information (Lindstedt and Naurin, 2010). It is often considered a universal remedy for all kinds of socio-economic, socio-cultural, socio-political and civic problems (Etzioni, 2010). Institutions gain the confidence of the public by ensuring that the demand and supply of information continue to flow and also by promoting mechanisms that access to information (Heald, 2012). Several denominators across different domains have offered various definitions and interpretations of transparency. However, there is no commonly concurred definition across different areas, except for a universal consensus that transparency is associated with public access to information (Bushman et al., 2004). One way to understand the meaning is to review a few broad general definitions of transparency. For example, in physical terms, transparency is a characteristic of a material object to conduct light and make other objects easily observable (Alzetta, 1997). In fiscal economic terms, transparency is defined as governments being open towards the public about structures and functions, policy intentions, public sector accounts, and projections (McCarthy, 2007). In the social sciences, transparency connotes the ability of interested parties to see through otherwise private information (Williams, 1999). Moreover, within the area of information technology, transparency is viewed differently and considered as implying to the actions of openness and accountability (Aslam, 2014). The practice of transparency comes in many different forms of varying commitments, engagements and obligations; thus, it is crucial to identify the categories of adopted institutional practices that are intended to promote transparent operations and the manner in which they are deployed. In the upcoming sections of this chapter, the pivotal transparency categories (such as proactive and reactive) and the deployment types (opaque and explicit) will be covered.

4.3 Cloud Security Transparency

Transparency is an essential means for strengthening information disclosure and enhances users' trust in using cloud services. It is one of the fundamental aspects of operations that ensure visibility regarding some important areas such as performance, configuration, billing, and workload (Aslam, 2014, Kalloniatis et al., 2013). Transparency in the past was particularly used to imply cloud customers' need for visibility on matters such as pricing models, but a broad range of interests such as security, service delivery and performance are now associated with the term. Security transparency, among all other spectrums, has prevailed as the most censorious necessity due to the complex chain of interactions between multiple actors, which fundamentally calls for the need to know how security and compliance measures are being applied to protect sensitive assets (Pauley, 2010).

4.3.1 Definition of Cloud Security Transparency

Considering the apparent definitions and connotations of transparency as attempted by researchers from different spheres of activities, for this research, cloud security transparency is defined as ***the disclosure of information relating to the security practices and management of virtual and application resources in the cloud to help customers in monitoring, verifying and tracking their data across cloud infrastructure. Cloud security transparency establishes the trustworthiness of the operations of the cloud service provider by enabling security monitoring, incident detection, reporting and management from the customer side.*** It has the potentials to establish trust and help customers to make informed decisions, achieve security goals, and operate in compliance with requirements.

4.3.2 Areas of Focus for Security Transparency in Cloud Environment

The cloud environment is composed of complex domains and resources that make achieving complete security transparency an enormous task. Visibility in every domain of the cloud cannot be efficiently and reliably provided due to certain restrictions or controls that may require the CSP to conceal particular security or configuration information. However, from the context of this research, some of the cloud domains where security transparency is achieved include:

- **Authentication:** Cloud security transparency makes possible the establishment and sharing of information regarding how end users are authenticated, granted or denied access to data and applications.
- **Access Roles and Duties:** Organisations usually define roles, layers, responsibilities and security levels associated with assets. Based on these specifications, information is shared and logged within an organisation in a manner that shows every task or activity executed against a particular asset.
- **User Account:** By security transparency, access attempts to authorised user accounts are consistently tracked, monitored and the information shared with an organisation to ensure every system access reported.

- **Security Policies:** Security policies are part of the control objectives that define how an organization's assets are used and make the provisioning of cloud service under the business and security requirements. An organisation establishes appropriate security policies that are enforced throughout the contract lifecycle. Violation of security policies ought to be transparently shared or communised with the organisation.
- **Infrastructure Security and Location:** Security transparency enables the sharing of the physical access, security and location of infrastructure that host or process organizational data such as data centres, servers, network tools etc.
- **Data Security:** Information relating to the implemented tools and processes designed to protect sensitive data is shared with an organisation employing security transparency. Transparency in this aspect mainly focuses on information relating to a user without the risk of compromising the data of other users.
- **Security Standards:** Standards usually allow an organisation to follow consistent stipulations for ensuring the safety of IT infrastructure and assets. Security transparency also enhances the sharing of information in this regard by enabling CSPs to share information on compliance with the regulatory bodies that regulate apply to their operations.

4.3.3 Why Security Transparency in the Cloud?

One of the most considerable obstacles to successful cloud migration is the management of security that is relatively aggravated by the non-transparent nature of CSPs to disclose security-related information associated with their offerings (Pauley, 2010). Users are driven by the fear of undisclosed security events cognate to on-going provider control procedures, and they always endeavour to make informed decisions by relying on disclosures to achieve optimum security goals and operate in compliance with requirements. Successful adoption of cloud technology by corporate users, businesses and organisations require a clear-cut disclosure of the security policies, designs and practices of CSPs, including on-going visibility of relevant security measures. These requisites for transparency constitute the pathway for users to assess the possible risks of cloud computing and its potential impact on assets. For example, a CSP may choose to outline the policies and procedures being employed to ensure the availability of user data by disclosing information on the architectural setup of backup plans, business continuity and redundancy strategies that provide continuous data availability. Security transparency in public clouds is considered as demanding a substantial magnitude of interest in comparison to other deployment models, due to its characteristics of being open to the public and serving a broad customer base. In contrast, other deployment models such as private clouds are designed explicitly for individual organisations, thereby offering customised functionalities that do not necessitate transparent operations.

4.3.4 How Security Transparency can Support Businesses

The ability of any organisation to recognize and adequately manage risks plays an important part, and the value of services and operations delivered to customers and other stakeholders. Security

transparency enables an organisation to identify their current and future requirements as well as providing a roadmap for aligning such requirements with cloud services. A broad spectrum of security solutions that support the core business processes and operations can be quickly established, including the identification of platforms and solutions that support the data security strategy of a business venture. By following a successful security transparency approach, an organisation can overcome the burden that often exists between information security strategy and business strategy objectives by directly aligning businesses processes and the security requirements that protect data. Also, the effective management of the risks associated with business data residing in the cloud requires the understanding of the level of risks, identification and prioritisation of sensitive data. In this direction, security transparency supports comprehensive classification efforts within organizational function or line of business, by leveraging automated tools that track data across cloud repositories including databases and applications.

Another notable point that highlights the essentiality of security transparency to business is the role it plays in the assessment and definition of realistic, attainable business strategies and performance goals. Organizational strategies outline how objectives are achievable, while goals express objectives to a perceptible and possible level. Factors such as technological posture, operations and organizational culture determine the objectives of an organisation and those that can be reasonably accomplished. As such, security transparency allows an in-depth understanding of an organisation's objectives and goals hierarchy, by directly establishing risk-based plans to support the monitoring of assets, as well as improvement opportunities concerning designing and operating an effective control process that is most consistent with their goals. Such improvement opportunities can take various forms including maintaining a robust control environment to support organizational initiatives that in return improve security; identification of focal risks that meet the organisation's risks appetite, including operational risks, business risks, technology risks and many other areas that pose significant risks of concern. In general, security transparency supports these processes through evaluation, recommendations to management, and reporting of incidents to relevant organizational stakeholders.

4.4 Properties of Cloud Security Transparency

Cloud security transparency is an essential aspect of the cloud that is underpinned by other important prerequisite properties (Chung et al., 2012). A conceptual understanding of the properties related to security transparency is highly imperative due to their significance in determining what constitutes transparency. Researchers (such as (Cappelli et al., 2010, do Prado Leite and Cappelli, 2010, Frentrup and Theuvsen, 2006) have identified some fundamental properties they perceive to be the founding blocks of security transparency. Cloud Accountability Project (A4Cloud) (A4 Cloud, 2017) has built methods and tools that contribute towards bringing CSPs and customers together in chains of

accountability for data protection in the cloud (Pearson et al., 2012). The primary objectives of A4Cloud include enabling CSPs to give their customers appropriate control and transparency over how their data is used; monitor and check compliance with customers' expectations; enable users to make choices about how CSPs may use and protect their data, and ensuring accountability. Hence, within this project, A4Cloud has identified and decomposed some fundamental properties that are relevant for measuring transparency and accountability. We perceive these properties as fundamentally influential in the delivery of security transparency, and thus, this paper has adopted some of such properties in addition to others for forming the basis for our approach. A justification for adopting the provisions of A4Cloud Project is based on the facts that it is a renowned industry project that strongly influences accountability, trust and privacy standards, which are significantly related to security transparency.

1. ***Auditability:*** Auditability refers to the ability of a CSP supported mechanism to provide security audit logs or information in a verifiable and accessible manner. Auditability is vital for customers to perform a periodic examination and verification on assets independently, and for determining how asset requirements are being met, who has accessed assets and how requirements are being managed or protected against risks. Auditability also ensures that security events relating to customers assets are consistently logged, and determines whether a CSP provides a stable balance between security controls and customers' needs requirements.
2. ***Accountability:*** Accountability constitutes the acceptance of responsibility for the protection of assets between the CSP and cloud customer. It ensures that the obligations to protect data are clearly established and observed, particularly between the CSP who oversees security protection and the cloud customer who stores and process data in a CSP environment. Accountability creates the necessary commitment that requires CSPs to act as the responsible steward and takes responsibility towards safeguarding, managing and ensuring appropriate use of cloud customer assets, as well as being accountable for any misuse of cloud customer asset.
3. ***Assurance:*** This is another vital component of security transparency that relates to the ability of the CSP to perform and fulfil specific or predefined security requirements of the cloud customer, as well as providing the confidence that security controls in the cloud environment will function as intended.
4. ***Monitorability:*** Deals with the provision of automated processes for collecting and analysing information for the detection of suspicious activities or unauthorised changes to cloud customer requirements. Monitorability provides cloud customers with the capabilities to consistently identify or be alerted of any security breaches and risks to their assets residing in the cloud.
5. **Verifiability:** Verifiability relates to the ability of cloud customers to independently validate or verify the implementation of security controls being supported and based on evidence provided by the CSP. It also relates to ascertaining how the CSP meets predefined cloud customer security.

4.5 Barriers to Transparency

The notion of transparency has gained significant prominence across all human endeavours because it leads to greater accountability and often enhances trust. However, despite the benefits gained through transparency, several barriers can affect the delivery of transparency. Some of the obstacles of transparency identified in the literature include (Fox, 2007, Naurin, 2006):

- **Biased information:** the partisan release of information that is non-objective or influenced by intrinsic motivation
- **Opacity:** releasing information that is obscure in meaning, to intentionally mislead customers and affect their decision making
- **Inaccessibility:** deliberate isolation of information, making it too difficult to access facts that influence customer decision making
- **Secrecy:** conscious concealment of information to specific customers
- **Unequal access:** depriving certain customers' access to information in the same quantity and quality offered to other customers.
- **Immaterial information:** providing customers with information that does not serve the intended purposes for which it is sought.
- **Spinning**: providing customers with information that is biased and only favouring the CSP.

4.6 Principles of Security Transparency in Cloud

It is necessary to provide some guiding principles that are imperative for understanding security transparency. The justification for these principles is to establish the fundamental norms that represent what is desirable and affirmative in the general sense of information disclosure within the sphere of cloud computing. In other words, these principles govern the action of providing visibility and to inform cloud actors about the precepts they are expected to uphold in the delivery of transparency. These considerations impact the accessibility and quality of information released under a transparency initiative. According to Kosack (Kosack and Fung, 2014), there are some general guiding principles for transparency. Our research will adopt these principles and tailor them according to the cloud-based systems.

- **Availability**. Availability means that information relating to occurrences regarding migrated assets should be available to the users. A monitoring system should be configured to stream real-time or near-real-time status information regarding customer assets and every action performed to those assets.

- **Clarity**. Implies that information should be clear and precise for easy understanding. In other terms, clarity eliminates all elements of ambiguity so that information is delivered precisely, in a coherent and intelligible manner. The benefit of clarity is about helping a company utilise

information to reduce complexity and uncertainty so that analysis can be applied to identify a clear path forward. An example of this is represented by a scenario where a shared responsibility model for security provisioning is adopted. The CSP should clarify their responsibility in securing cloud infrastructure, while a user should take on the responsibility of securing data or applications integrated into that infrastructure.

- **Current**. Means that the information should be up-to-date. Information should be regularly communicated to customers in real-time or near real-time flow for enabling the evaluation of actions about customer assets in the cloud. Also, the information should clearly state the timestamp and occurrences of activities about cloud-hosted assets. For example, anomaly detection in the cloud environment much depends upon current or real-time information.

- **Relevance**. Information should be relevant to the context. Cloud systems consist of numerous virtual machines, hardware, operating systems and applications that provide valuable information. A disclosure must be pertinent to provide information from a variety of platforms. For example, if a company subscribes to information feed on cloud resource availability, the usage data of the cloud resource considered should be particularly shared with an organisation.

- **Notification**. Information relating to security incidents, events, deviations, or occurrences that affect customer assets in the cloud should be appropriately disseminated to concerned customers so that they can evaluate the occurrences and optionally take action. For example, the presence of dedicated monitoring systems that detect security phenomenon and notify an organisation to take remedial actions or invoke an autonomous action.

- **Verifiable:** The information generated by the CSP can be easily verified through supporting evidence, testing or any other form of analysis.

- **Free of Charge or at Low Cost**. Information should be automatically compiled, organised, collocated and streamed to concerned cloud actors that subscribe information feed for free of charge or at a low cost.

4.7 Categories of Cloud Security Transparency

It is reasonable to identify the common categories at which security transparency is actualised in cloud lifecycle. The significance of this is to elaborately underline the situations where CSPs tend to be transparent and provide some clarity into how transparency is perceived. For instance, cloud users usually make cloud migration decisions based on public information (freely available to all in public domains) where a provider is unlikely to provide detailed information due to security concerns or privacy restrictions. More accurate and all-encompassing information (in individual contracts) is often provided when agreements are reached. Supposing the private information is the most critical and

relevant for decision and it is only made available after agreeing on a contract, the tendency this generates is that users might wrongly perceive the public information as being misleading or deception from the part of the CSP. We, therefore, classify the various forms at which transparency is articulated as shown in Figure 4.1

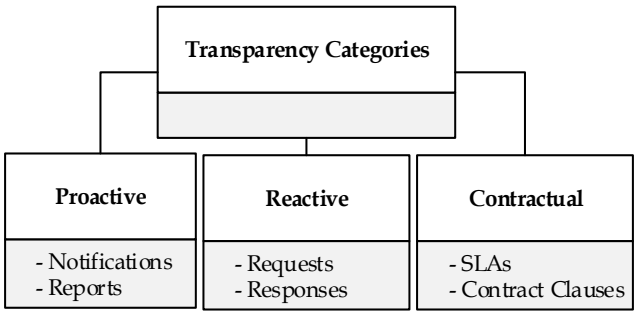

Figure 4.1 Categorisation of Cloud Security Transparency

- **Proactive Transparency (Voluntary):** Otherwise referred to as voluntary disclosure, stems from CSPs initiatives to make rudimental security information of their offerings available to the whole public without a request being filed, and the aim is to generate assurances using a multiplicity of methods ranging from notifications to reports (through mediums such websites and portals, benchmarks, whitepapers etc.). This disclosure is generally intended to uplift customer trust and confidence, assist customers to evaluate basic CSP control environment, demonstrate CSP conformance to regulatory or industry requirements, and also helps customers address some specific questions around general cloud computing practices. It does not reveal information that could jeopardise the security posture of a CSP or expose them to harm's way. For instance, when a cloud user's data falls under restrictions emanating from regulatory or compliance requirements, the choice of a CSP hinges on the contentment that the provider is fully compliant to the regulatory body; otherwise, there is the risk of violating regulatory, legal or other privacy requirements. The CSP counteracts customer contemplation through proactive disclosures to illustrate controls and certifications that reveal the reliability of their services at the preclusive cloud strategy stages. The benefits that accrue from CSP's initiative to proactively disclose information are numerous. It ensures that cloud users are enlightened about the security management procedures applied to their resources while in the custody of the CSP. From another perspective, the ready availability of information ensures timely access to information that helps ensure the equality of access to information for all cloud customers including small, large and medium enterprises without the need to file special request, which is indeed associated with various sort of commitments. However, a supposed downside of this disclosure type is the possibility of a CSP to disclose inherently limited information, attempt to conceal damaging information that could tarnish its reputation, or even proclaim deceptive controls that give an impression different from the genuine environment.

- **Reactive Transparency (Necessary):** Reactive transparency emerges from a request-response routine at the initial procurement phase between an organisation and the CSP for the latter to provide additional information. It may arise from legal or regulatory requirements that mandate CSP to disclose certain information during contract negotiations. Through a request-response routine, a prospective cloud customer files requests for and receive information from an existing CSP. This mainly takes shape through two procurement methods, i.e. Request for Information (RfI) and Request for Proposal (RfP). To demystify the meaning behind each of the terms, RfI is a request to several potential CSPs to specify conditions, information gathering, or for cloud strategy purposes. It is mainly used when a cloud user has not identified their security requirements and need more information from a CSP to help them discover what steps to take next before negotiations commence. While an RfP is mainly employed when a cloud user has determined the scope of their security requirements or identified inherent cloud problems but is unaware of how to solve them, the CSP analyses the customer's security requirements and responds with the actual existing alternatives in their offerings. Ideally, the RfP reflects the strategy, short and long term requirements of the customer while seeking specific information, security offerings and particular items which the CSP is proposing. Generally, the contents of a CSP response represent the actual settings or state of their offerings, rather than a meagre attempt to beat competition from other vendors, which indeed generates transparency into how individual requirements are distinctly addressed. The advantage of the request-response driven approach is its ability to enable cloud users exclusively specifies their security requirements for assessment and the identification of suitable controls by the CSP. However, it could be argued that it has become a traditional practice for CSP's to publish frequent solicitations in public domains so that future cloud users do not have to file a request, saving time for both the CSP and the customers.
- **Contractual Transparency (Statutory):** This implies a valid written agreement between a CSP and a customer where the provider observes complete disclosure of all essential security services strictly relevant to a particular cloud user while refraining from divulging information that could compromise the privacy of other customers. Service Level Agreements (SLAs) are useful tools widely used by both CSPs and their customers as a channel for ensuring transparency and establishing a common pact to manage the security requirements requested by a customer and the security levels being offered by a CSP, which becomes legally binding. Also, the SLA forms the basis for defining responsibilities and the remedies available for customers in case of a contract breach. The information contained in SLAs is usually broader in coverage than those found in proactive and reactive transparency schemes. The Fundamental aspects of the SLA are the representation of the contexts shared by the two actors, and how each actor utilises the contexts in its operations throughout the SLA lifecycle. In other words, the SLA provides a comprehensive description and transparent security processes for both the

CSP and customer to avoid uncertainty, apprehension and disputes. Conventional SLAs generally provide clarity on CSP service offers, unambiguous definition of expectations and obligations on both sides, and the boundaries of liability. Nevertheless, a notable limitation to this class of transparency is that essential security property of a customer may remain uncaptured. But despite this limitation, it still provides critical salient characteristics that support customer's consideration for (i) security governance, legal and regulatory requirements, (ii) and allows customers to determine the impact of CSP offerings on business processes, including those changes required to enable the cloud services to be effectively useful to operate objectives.

4.8 Cloud Security Transparency Deployment Practices

Cloud security transparency works as a mechanism that contributes to improved operations and fosters the trust-building process among users. Information that is disclosed through the performance of transparency takes different dimensions. Some information disclosure eminently supports the cloud community in decision making while, in some cases, certain disclosures present inessential information that perhaps generates ambivalence. Thus, the idea of cloud security transparency can be unpacked from different dimensions as identified by Jonathan Fox (Jonathan Fox, 2010). It mainly falls into two categories: opaque and explicit transparency as illustrated in Figure 4.2:

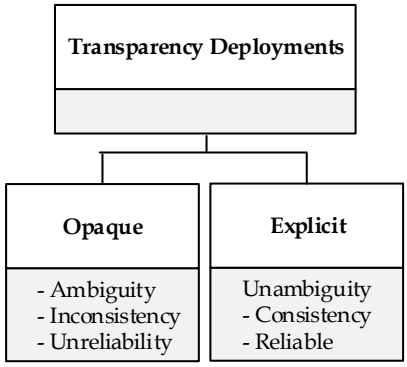

Figure 4.2 Cloud security transparency deployment practices.

- **Opaque Transparency**. Opaque transparency means that information is not well clarified. It involves CSP disclosing information that either partially represents its actual operational values or provides equivocal statements. It may also include inconsistent or unreliable information in terms of how controls are actualised in the cloud environment. For example, a CSP might claim to operate a service with security as a key principle through the implementation of consistent technical network security routines but then fails to genuinely demonstrate the application or actual implementation of significant secure network architectures and security devices that monitor and control communications at the key

boundaries within their environment. This would mean that transparent service is provided with virtually futile effects.

- **Explicit Transparency**. refers to the disclosure and dissemination of information that represents a realistic implementation of CSP security control that precisely outlines the processes and procedures of how operations are securely managed. It provides a comprehensible elucidation on the CSP's approach to ensuring the protection of company assets while in their control. This type of transparency is considered as most effectively attracting customer trust and confidence, as well as supporting accountability in the cloud. An example of explicit transparency would involve a CSP supporting a system that collects data related to the state or behaviour of customer assets and sends such data for onward analysis and evaluation by the concerned customer.

4.9 The relationship between Categories of Transparency and Deployment Practices

An overlapping relationship could be identified as existing between the transparency categories and its deployment practices. It could be argued that some CSPs provide the actual information that corresponds to their environment, while a proportion plausibly opt to provide false information to keep step with market competition, and others may attempt to conceal certain damaging information that could affect their reputation.

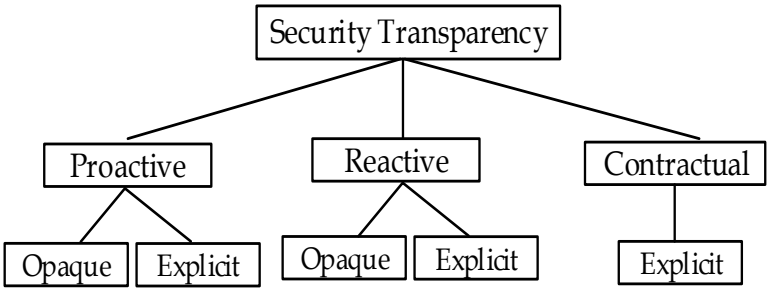

Figure 4.3 Relationship between transparency categories and deployment practices.

Figure 4.3 illustrates how each security transparency category is associated with one of the two deployment practices. For instance, a CSP may proactively provide transparency through security whitepapers regarding the security and compliance measures they have in place to protect customer assets. The CSP, nonetheless, may deploy an explicit security transparency practice to provide detailed information into their existing monitoring and prevention controls that prevent attacks, malware and other unauthorized activities while refraining from disclosures that expose them to risks. However, it may choose to deploy an opaque transparency practice to state the existence of security controls that either fail to capture the actual state of controls or are presented in an ambiguous form. Moreover, contention in this regard upholds the opinion that contractual security transparency is mainly associated with explicit deployment practice. This argument is supported by the fact that contracts are enforced by law and become legally bound once an agreement is reached between the CSP and the user. Thus, a

CSP is less likely to provide non-transparent or ambiguous disclosures that could result in ramifications and consequently lead to indemnifying its customers.

4.10 Summary

This chapter provides the fundamental properties and basics of security transparency. It presented a new definition of security transparency from a cloud computing perspective and essential areas of focus for security transparency in the cloud. Also, it offered the reasons for ensuring security transparency and how transparency can support businesses. The chapter also discussed the salient properties of cloud security transparency such as auditability, accountability and assurance, as well as the barriers that hinder transparency. Further, the principles and categories of security transparency are introduced which provide the basis for developing the CSTF. Importantly, the chapter introduced security transparency deployment practices that are also used in determining the level of security transparency offered by CSPs.

CHAPTER FIVE

Cloud Security Transparency Framework

5.1 Introduction

In this chapter, an overview of the security transparency and audit framework is presented. The term framework is often used in various domains such as information systems design, business process, and software engineering, etc. By definition, a framework is a holistic set of abstracted ideas or rules that can be used to deal with or solve a particular problem (Succar, 2009). From software engineering perspectives, a framework is defined as a set of classes that embodies an abstract design for solutions to a family of the problem (Johnson and Foote, 1988). In general terms, a framework is defined as a set of concepts that layout key factors, constructs or variables and the presumed relationship among them (Zachman, 1987).

The motivation for adopting a framework-oriented approach in this research is that it ensures a thorough elucidation and manageable implementation of conceptual ideas. It also helps in identifying and connecting conceptual components to ensure consistency, efficiency and effectiveness, as well as identifying interrelationships between these components. Therefore, the cloud security transparency framework presented in this chapter provides a logical representation and interrelation of salient concepts that are necessary for the implementation of a conceptual remedy. It follows three different levels of abstraction along with associated concepts within these levels. These levels build the bridge from the concepts necessary for transparency with the organizational settings and technical means for implementation

Additionally, the framework incorporates many techniques for enhancing security transparency and concentrates on providing a comprehensive means for auditing assets outsourced to the cloud. It takes a high-level set of concepts, decomposes and associates them with each other to provide a level of detail that allows for clarity in implementation. To achieve coherence and consistency in the framework, concepts are modelled using a renowned methodology for requirements engineering called Secure Tropos (Mouratidis and Giorgini, 2007), that is based on the *i** modelling (Yu, 1997), which uses the concepts of actors, goals and social dependencies for defining the obligations of actors (dependees) to other actors (dependers). Secure Tropos contains concepts such as constraints, security constraints, secure dependencies, secure goal, etc. In this way, concepts from Secure Tropos are considered and extended in identifying and forming concepts for the framework.

In addition, a common vocabulary that is based on ontologies is used, which provides a reliable solution to achieve the desired objective of the framework. Ontology is defined as an explicit specification of conceptualisation that can be looked at as an abstract, simplified view of the world that is to be

represented by some purpose (Gruber, 1993). Ontologies are generally used for two purposes: for knowledge representations and knowledge retrieval. Ontologies also provide supplementary benefits such as reuse of domain knowledge, making domain assumptions explicit, and to analyse domain knowledge (Spyns et al., 2002). The ontology-based approach enables the definition of concepts and their dependencies in a more understandable way. In summary, the reasons for the ontological approach in the framework development are: ontology ensures coherent conceptualisation of real-world domains; it enables the specification of the semantic relationship between various concepts; and provides a common understanding of the structured association between different concepts.

5.2 Approach to Framework Development: Levels of Abstractions

The proposed framework approaches to cloud security transparency from three different levels of abstraction — a conceptual view, organizational level, and finally at a technical level, as illustrated in Figure 5.1. Sitting at the top level of abstraction is the conceptual view that establishes and defines the various concepts that constitute security transparency in cloud computing. This layer aims to introduce a high-level elucidation of the foundation concepts that underpin transparency, which is indeed valuable for helping organisations have a comprehensive understanding of how cloud security transparency can be implemented at subsequent levels from an organizational and technical perspective. At the middle layer lies the organizational level, which is triggered by the concepts developed at the conceptual level. It introduces other vital concepts that are mapped at an organizational setting. In other words, the organizational level describes how the fundamental concepts formulated at the conceptual view are associated with other concepts from organizational perspective for ensuring an organisation's attainment of security transparency. Lastly, the technical layer that lies at the bottom of the framework deals with the implementation of the conceptual view and the concepts at the organizational level from a technical outlook. The layer specifies the technical outlook in terms of the practical development and implementation of security transparency using audit technique using the concepts identified in the previous layers. The levels of abstraction influence each other and they are related in a way that supports the mapping of all the concepts at each level.

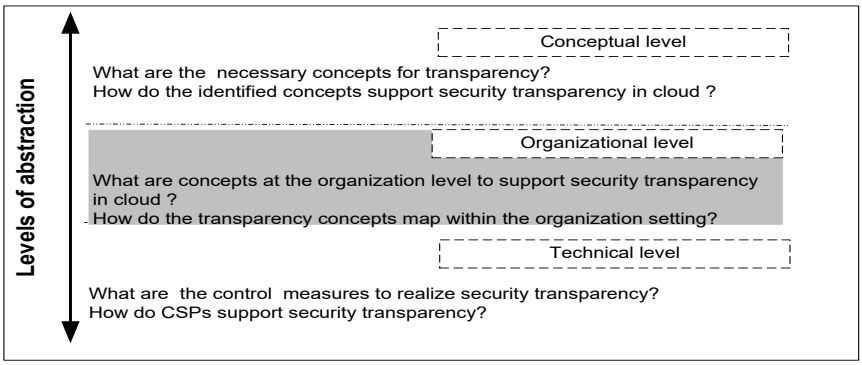

Figure 5.1. Levels of abstraction for security transparency in the cloud.

5.3 Conceptual View

Conceptual view implies the clear interpretation and explicit deconstruction of the abstract ideas or concepts needed to understand what a framework is, systems or components, what it does, how it addresses specific objectives, and how it is best used (Chen, 1976). The conceptual view attempts to accurately and precisely provide a meaning for and model the concepts in such a way that people without high-level knowledge can understand what constitutes security transparency. It also provides the essential foundation concepts that are used for the development of security transparency at organizational and technical levels. Regardless of the category at which it is articulated and the deployment practice being followed, it is paramount that security transparency encompasses factors that support its development and delivery between cloud actors. The identified concepts are given below:

5.3.1 Actor

An actor represents an entity (an organisation, a person or CSP), that participates in a process, performs a task, or carries out an action in cloud computing service delivery and consumption (Castro et al., 2002). In other words, actors could be an organisation, functional department or people that are involved in providing, requesting or receiving transparency through many forms of information exchange. Actors are related and interact with each other in one or many ways. For example, an organisation can be an actor with many other actors such as staffs and clients that use the services provided by the organisation. The interaction between actors is established by factors such as delivery and consumption of services, exchange of information or the provision of supporting computing needs. The increased service orientation and the opportunities of service offerings offered by cloud computing platforms, as well as the emerging opportunities to integrate different cloud service components to create value-added chain have given rise to a set of new roles within the cloud realm. The information about actors and the nature of their relationships and interactions need to be identified and documented. The dimension of importance includes considerations such as the role played by each actor. This information is needed to interpret, manage and process the actor's input. To provide an increased level of details, five major actors have been identified.

5.3.2 Transparency Request

Security transparency is viable when actors are supported to make decisions based on the information provided by the CSP. The purpose of transparency request is to allow an actor to seek for and receive information about: the capabilities of another actor to fulfil requirements, the efficacy of an actor controls, and the events or incidents that affect migrated assets within the cloud environment. Transparency request is initiated by an actor seeking real-time, log data or documented information about cloud systems and operations, particularly information that discloses how actor's requirements can be fulfilled and how operations are being carried out. The core of this concept is enabling an actor to wholly seek and collect information needed to support their operations, thereby constituting the need

for an explicit rather than opaque transparency. In most cases, actors (CSPs) exclusively deploy transparency mechanisms such as web portals as a means of making information about its operations available and which can satisfy transparency requests initiated by organisations. It is noteworthy to highlight the distinction between transparency requests and requirements concept (at an organizational level). Transparency requests do not independently support the description of the organisation's requirements; it rather solicits details on how requirements are fulfilled and how incidents or events that affected organisation's assets are reported; whereas, the requirement concept aims at enabling the specification of the most relevant security requirements to the assets of an organisation.

5.3.3 Mechanism

A mechanism is defined as the communication platform being adopted for the provision or disclosure of relevant security information about an actor's operational processes. The term is used to imply an actor using initiatives such as security and audit reports to make operational, technical or procedural information available, detailing how it conforms to governing rules and ensuring security controls. Furthermore, a mechanism is predominantly the fore attribute that triggers the conceptualisation of other concepts because it presents first-hand information in areas of standard security practices and management of cloud services.

5.3.4 Evidence

Evidence refers to the submission of relevant electronic, documentary or other specific reports that are provided by an actor to substantiate its transparency mechanisms. The aim is to enable the actor to produce any forms of system, user, or application activity reports and on the general security status of organisation assets within the cloud environment. Another crucial aspect of the evidence is to support actors to perform a check and verification of disclosures against their transparency needs to purposefully determine the integrity of an actor's response to requests.

5.3.5 Accessibility

Information accessibility is paramount in achieving transparency and it focuses on the ability of actors to access meaningful information relating to cloud controls, operations and satisfaction of requirements. Transparency cannot be achieved if an actor withholds information from other actors. Therefore, accessibility encompasses the degree to which an actor can easily locate information. It also involves the credence for an actor's transparency mechanisms and evidence to be made requisitely available, accessible and locatable to all organisations. While making information accessible, CSPs must ensure that the quality of information is maintained and free from problems such as err, bias, and incompleteness.

5.3.6 Liability

This is the state of being legally responsible for the provision of transparency, i.e. an actor becomes legally answerable for the contents of information supplied to other actors. An actor that is held liable for disclosure becomes lawfully responsible for rendering agreed redress in non-fulfilment or misstatement of information. For example, if contractual agreements have been reached between a CSP and an organisation for the former to provide 99% service availability, they become legally liable to ensure such and redress the organisation in the event of a failure to meet the target.

5.3.6 Monitoring

This is the ability to observe and check the quality of the information provided. To substantiate the accuracy of disclosure, it must be observable by other actors by, for example, analysing evidence generated by a transparency mechanism being supported by an actor. In other words, monitoring is a function of processes that can be used to establish the effectiveness of the internal operations of an actor by observing the content in evidence.

5.3.8 Verifiability

This is the degree to which disclosure can be confirmed to be existent and to establish its accuracy. This concept allows other actors to validate whether observable properties comply with agreed expectations or requirements. It ensures that the materials presented are made truthfully and reflect genuine credibility about perceived quality.

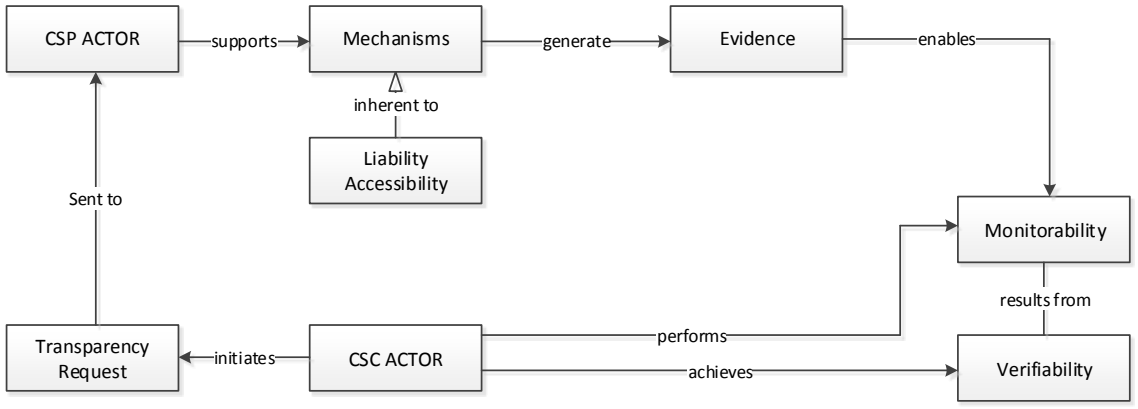

Figure 5.2 Conceptual Model of Cloud Security Transparency.

Figure 5.2 provides an insight into the conceptual view of security transparency. An actor (an organisation) initiates a transparency request to another actor (CSP) soliciting for transparency on their operational practices, security controls, and the overall cloud service environment, relating to assets and measures taken to fulfil requirements. The CSP, on the other hand, supports mechanisms for transparency as a way of making vital information regarding operational processes available. A mechanism is characterised by various means for information disclosure, which is literally used to

disclose customary security practices and the status of customer assets within the cloud environment. The responsibility to support a mechanism may either be one-sided or shared amongst the two actors. This is commonly noticeable in situations, for instance, public clouds where a CSP is responsible for supporting mechanisms of transparency, whereas in specific setups such as private clouds an organisation is solely responsible for security administration and control of information.

Additionally, the mechanism generates evidence to provide status reports on the condition of the CSP environment and assets belonging to an actor. For the evidence to yield significance, it must possess the qualities of being monitorable and verifiable for establishing the genuineness or truthfulness of disseminated information according to the perceived quality and expectations of an actor. Therefore, the organisation verifies the transparency mechanism through monitoring, thereby providing the avenue to verify disclosed information.

5.4 Organizational Level and Ontological Modelling of Concepts

The organizational level is based on the foundation concepts identified at the conceptual level. It is intended to ease the implementation of security transparency at the technical level. For example, an organisation at the conceptual view initiates a request for transparency demanding additional security information about the CSP's security practices. The CSP responds to such a request by disclosing information through mechanisms for transparency such as independent third-party audit reports or security whitepaper. Before the request for information is sent, an organisation ought to apply some essential analytical steps such as: identifying their goals, assets and requirements, etc. The adoption of a common terminology of the concepts at the organizational level will help in understanding the concepts and the overall implementation of the process. A good starting point for establishing and elaborating these concepts in detail is through the application of ontology-based conceptual modelling.

Ontology enables the conceptualization of a specific domain of interest into machine-readable form (Giaretta and Guarino, 1995). It is as defined by Spyns et al (Spyns et al., 2002), as the description of knowledge as a set of concepts within a domain and the relationship that holds them together. In other definition, ontology is an entwined hierarchy of concepts that presents an explicit description of concepts within a particular domain, related properties describing various features and attributes of the concept, and restrictions (Antoniou and Van Harmelen, 2004). An ontology may be domain-specific, i.e. addresses a specific aspect of a domain, it can also be task-oriented for achieving a particular task, or it may be generic with a focus on high-level concepts (Stevens et al., 2000). In terms of application, an ontology can be used as a basis for software development, as common information access for humans and applications or as an application-neutral knowledge base (Stevens et al., 2000). The complexity of ontology varies, from a vocabulary that consists of a list of concepts to logic-based knowledge that

contains concepts, instances, relations and axioms for providing reasoning services (Lambrix and Tan, 2005).

The organizational level comprises many concepts that are built upon the concept of actors, goals, threats, risk analysis, requirements etc. Ontology is used to provide an explicit knowledge-based understanding of the attributes, relationships, restrictions and rules between the concepts. The ontology is supported by formal semantics for knowledge representation using rules and logic-based formalism that aim at laying the basis for automated deduction. Such formalisation eradicates vagueness and ambiguity, and thus ensures consistency for computational purposes.

One of the fundamental logical formalisation techniques used for knowledge representation is first-order logic (Smullyan, 2012) and it is chosen in this thesis to present logic as a form of knowledge representation for the concepts of security transparency. The benefits of first-order logic are that it allows the description of concepts, objects or things that have an individual identity, and to construct logical formulas around these objects using predicates, variables, functions and logical connectives (Russell and Norvig, 2016). This means that natural language statements or rules regarding the concepts can be expressed in terms of coherent sentences with appropriate predicate and function symbols.

By using semantic rules and logical representation for each concept, the focus is placed on the graphical visualisation of the ontologies to aid their assessment and analysis. One technique that can be used is graph visualisation, which supports comprehending the structure of ontologies. Hence, Protégé is used to graphically visualise the ontologies because it provides an intuitive editor for ontologies and other extensions for ontology visualisation. Protégé is one of the most widely used free, open-source ontology editor that was developed at Stanford University (Noy et al., 2001). Using Protégé, concepts of the security transparency framework are organised in a generalisation hierarchy through “is-a” links (inheritance). Each concept consists of zero or multiple sub-concepts. Also, each concept has an object (relationship) and data (characteristics) properties to describe the various features of the modelled concepts.

5.4.1 Actors

The elucidation of actors provided at the conceptual level produced a broad or general meaning of actors that are not specific to any context. However, the demotion of actors at the organizational level takes a different purpose by focusing on the roles played by various entities based on a specific context. Therefore, actors are the entities whose interests are taken into account at the organizational level. It is a pivotal activity that yields useful and accurate information about the individuals or group of people that are involved, have vested interest or play a vital role within an organizational context. Actors are

highly significant in enabling an organisation to manage the process of the framework, as well as preventing potential misunderstandings or conflict of interest. In general, an organisation must identify actors that are actively involved from both within and outside including the role played by each actor. Organisations usually have different types of actors with different interests, duties, tasks and priorities. Actors are identified according to internal and external actors. Internal actors are people who are committed to serving the organisation such as an information security analyst, the board of directors, etc. External actors are entities outside an organisation such as the CSP who provide various forms of computing services. The listing of actors varies and will be determined in every organisation according to its volume of activities and resources.

Table 5.1: Rule-Based Knowledge Representation of Actors

[∀x.(actor(x) → ∀x(can be(x,y) ∧ internal(y)) ∧ external(e))]
[∀x.(InternalActor(x) → ∀x(can be(x,a) ∧ keyPersonnel(a)) ∧ tOPMANAGEMENT (b)) ∧ otherUsers(b))]
[∀x.(ExternalActor(x) → ∀x(can be(x,a) ∨ CloudProvider(a)) ∨ CloudBroker (r)) ∧ CloudAuditor(z))]
[∃x.(KeyPersonnel(x)→∀a(can be (x,a) SecurityAnalyst(a)) ∧ SecurityAuditor(b) → ∀z canPerformAudit (z,x))]
[∃x.(CloudProvider(x)→∀a(provides(x,a) ∧ IaaS(a)) ∧ (provides(x,b) ∧ PaaS(b)) ∧ (provides(x,i) ∧ IaaS(i))]

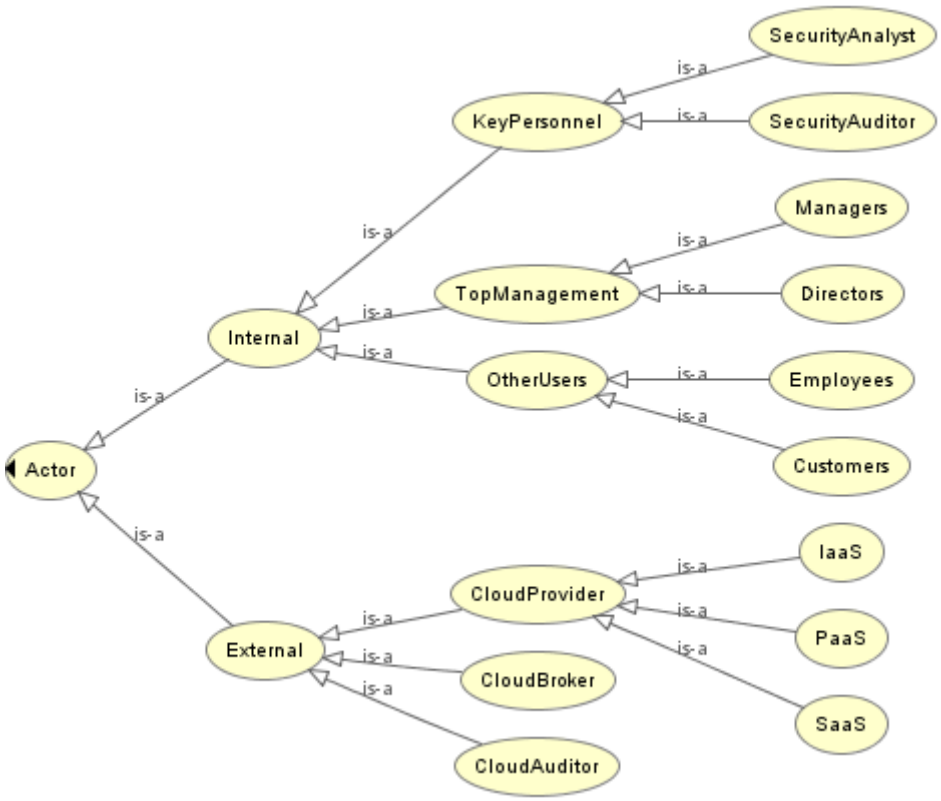

Figure 5.3: Ontology of Actors

5.4.2 Assets

Assets are any application or software owned by the organisation that is used in the course of executing or managing business functions. This concept involves the identification of an organisation's assets in

terms of the assets that are hosted in the cloud environment. Assets are profiled to include categorisation according to asset criticality, security goal and supported business function to the organisation. The relevance of this is to help the organisation to have a common, consistent, and unambiguous understanding of asset boundaries, clearly designated asset goals, a description of how the asset is stored or processed, and an opportunity to determine the asset's criticality. The asset has four important attributes:

Table 5.2: Rule-Based Knowledge Representation of Assets

[∀x.(asset(x) ⊨∀x(contains (x,a) → ∧ assetProfile(b,x)) ∧ Criticality (y,x) ∧ gecurityGoals (z,x)))]
[∀x.(SecurityGoal(x) ∃∀x(contains (x,a) → confidentiality(c,x)) → Integrity(i, x) → availability (a,x) → accountability (y,x) → conformance (z, x))]
[∀x.(Criticality(x) ∃!∀x(can be(x,a) ∧ high (h,x)) ∧ low (l, x) ∧ medium (m,x))]
[∀x.(AssetProfile(x) ∀x(consistOf (x,a) ∧ data(d,x)) ∧ hardware (h, x) ∧ software (s,x) ∧ businesProcess (b, x)))]
[∀x.(AssetProfile(x) ∀x(can be (x,a) ∧ ∀xdata(d,x)) ∧ transactional (t, d) ∧ metadata(m,d) ∧ master (s,d) ∧ logs (l,d)))]
[∀x.(AssetProfile(x) ∀x(can be (x,a) ∧ ∀xhardware(h,x)) ∧ network(n, h) ∧ storage(s,h) ∧ servers(v,h)))]
[∀x.(AssetProfile(x) ∀x(can be (x,a) ∧ ∀xsoftware(s,x)) ∧ vm(v, s) ∧ application(a,s) ∧ os(o,s)))]

Figure 5.4: Assets Ontology

- *Asset Profile:* describes the necessary descriptive and information about the many components of all assets belonging to the organisation. Assets are profiled in a register to give a clear understanding of all assets and their subcomponents.
- *Security Goals:* each asset has a specific goal that must be maintained in order to ensure the protection of the asset and conformance to secure behaviour. Asset goals are established using five key areas related to information assets, including confidentiality, integrity, availability, accountability, and conformance.
- *Asset Criticality:* criticality is the primary indicator used by the organisation to determine the importance of the asset to the business. The criticality of an asset category can be highly critical, moderately critical or low criticality. Assets are highly critical if they have the most valuable to the organisation, a moderately critical rating represents a moderate value; while low criticality means little value to the organisation.
- *Supported Business Process:* business processes are structured activities or tasks backed by assets to serve a particular business objective or produce a service or product. Each asset is related to the specific business function that it supports.

5.4.3 Risks

Risks are the potential events, activities or attacks that could potentially compromise the security of assets, security goals or business process leading to a loss or negative impacts. A Risk can affect an asset when vulnerabilities, flaws or weaknesses within the system or its environment can be exploited by threats such as natural or human factors to cause harm. The purpose of this concept is to identify the risks facing the assets, security goals and business process, as a result of threats exploiting the vulnerability. It also determines the likelihood of the risks to materialise and the potential consequences or impact of the risk attack. The risk concept also serves to provide a holistic overview of security measures that can be used in controlling or mitigating the risks. It consists of:

- *Threats:* threats are potential dangers that might exploit a vulnerability within the cloud ecosystem and cause possible harm to one or many asset components to deter security goals or hinder the business process. Each risk is associated with a specific threat, and the threats are categorised to evaluate their severity to assets. Also, threats are considered from different sources that elaborate more about security threats associated with cloud computing such as ENISA (European Network and Information Security Agency, 2009)
- *Risk Likelihood and Impact:* the likelihood of occurrence and the possible impact or consequences of risks to the organisation are determined. Risk likelihood represents the probability that a given risk will occur. Risk impact refers to the consequences and extent to which an organisation is affected if a risk is realized.

- *Control Measures:* security measures are the safeguards or counter-measures that must be implemented to avoid, detect, counteract or minimize the impact of risks to assets or business process of the organisation. Control measures are identified based on the recommendations of industry guidelines and standards. Primarily, CSC CIS (Centre for Internet Security, 2018) and ENISA (ENISA, 2016) are used to identify actionable controls measures.

Table 5.3: Rule-Based Knowledge Representation of Risks

[∀x.(risks(x) ⇒∃y.(contains(r,) ⇒ threatsProfile(p,x) ∨ riskRegister(q,x) ∨ controlMeasures(y,x)))]
[∀x.(threatsProfile(x) ⇒∃(has(r) ⇒ category(p,x) ∨ targetAsset(q,x) ∨ threatsname(y,x) ∨ threatID (q,x) ∨ severity(z,x))]
[∀x.(severity(x) → ∀z(canbe(q) → (low(q,x) ∧ medium (r,x) ∧ high(y,x))]
[∀x.(targetasset(x) → ∀z(canbe(q) → hardware(r,x) ∧ software (s,x) ∧ data (z,x))]
[∀x.(impact(x) → ∀z(affects(q) → businessprocess(r,x) ∧ securitygoals(s,x))]
[∀x.(controlmeasures(x) → ∀z(contains(y) → cnotroltype(q,x) ∨ specification (s,x))]

Figure 5.5: Risks Ontology

5.4.4 Requirements

Requirements imply vital security needs for safeguarding assets and enabling security transparency. Requirements also refer to a set of conditions, capabilities or quality features that must be provided or

satisfied by the CSP to ensure the security of cloud services hosting organisation's assets, achieving transparency, overall safety safeguard of assets and delivery of business operations. An organisation identifies and clearly defines the essential requirements that safeguard assets and which are vital to achieving transparency. Requirements are formulated from different dimensions and describe more concretely the essentialities that must be satisfied to assure the security of assets. Requirements are derived from industry standards and best practices such as CSC CIS (Centre for Internet Security, 2018), CSA CCM (Cloud Security Alliance, 2017a).

- *Transparency Requirements:* these are related to measures taken for establishing confidence about the existence of transparency principles and mechanisms that enable an organisation to verify whether assets are being safeguarded and cloud systems are working as intended.
- *Basic Requirements:* these are a set of actions that establish fundamental, specific and actionable procedures, or process for ensuring the safety of assets and prevention most pervasive risks.
- *Business Requirements:* these refer to a set of actions and procedures that ensure an organisation acts under a set of rules, policies, and comply with applicable regulations.
- *Operational Requirements:* these encompass a set of procedural, governance and administrative actions that are enforced for ensuring comprehensive operational security in a cloud environment.

Table 5.4: Rule-Based Knowledge Representation of Requirement

[∀x.(requirement(x)) ∀x(has(x,a) ⇒ assetProfile(q,x)) ∨ assetType(y,x) ∨ Controls (z,x)))]
[∀x.(requirement(x) ⇒ (requirementType(x,q) ⇒ operational(q,x)) ∧ business(y,x) ∧ transparency(r,x) ∧ basic (z,x))]
[∀x.(requirement(x) ⇒ (assetType(x,q) ⇒ application(q,x)) ∧ software(y,x) ∧ data(s,x) ∧ basic (r,x) process(z,x))]
[∀x.(requirement(x) ⇒ (Controls(x,q) ⇒ domain(q,x)) ∧ type(y,x) ∧ specification(q,x) ∧ ID(r,x)))]

Figure 6.6: Requirements Ontology

5.4.5 Assess CSPs

Before cloud migration takes place, a CSP's comparison and assessment exercise are used to guide the selection of a CSP amongst many commercially available CSPs with the sole aim of identifying a trustworthy CSP that provides sufficient transparency mechanisms and who have the assurances to satisfy requirements. The comparison and assessment mainly aim at assisting an organisation in matching their requirements to appropriate CSPs according to operational, business, transparency and basic requirements. The assessment also helps organisations to reflect on the CSP's security profile decision making.

- *Collect CSP Information:* information about CSPs security transparency profile and assurances are collected to support a judgement based on credible evidence of a CSP's transparency. Various information sources such as whitepapers, CSP whitepapers, etc. are used for information collection in respect of transparency, business, basic and operational requirements
- *Perform Assessment:* multiple CSPs are compared and evaluated according to a set of questions formulated in accordance with the principles of security transparency, a measurement metric and an equation that have been specifically designed to support the assessment. The criteria

consider security transparency types (opaque and explicit) that are assigned to CSPs for determining the type of transparency they provide.

Table 5.5: Rule-Based Knowledge Representation of Assess CSP

Figure 5.7: Ontology for Assess CSPs

5.4.6 Evidence

An Evidence takes two perspectives: the first involves affirmations from the CSP before cloud migration takes place, which specifies the existence of acclaimed security controls and transparency mechanisms that provide an overview of how customer requirements can be met, and which are needful for assessing CSP offerings. The other perspective of evidence is meant for supporting the security audit exercise, and evidence in this dimension represents data, records, assertions or additional information that is collected to conduct security audits and in particular, relevant to the requirement that is being audited. This type of evidence provides a reasonable basis for arriving at conclusions and forming audit

opinion findings. In general, the evidence presents a detailed representation of the actual control implementations by the CSP in the areas of transparency, business, operational and basic requirements for the CSP to sustain and meet organisation's expectations.

Table 5.6: Rule-Based Knowledge Representation of Evidence

[∀x.(evidence(x) ∀xfor(a) → securityaudit(y,x) ∧ beforemigration(z,x))]
[∀x.(evidence(x) ∀x(requires(r) → evidencetype(q,x) ∧ evidencsource(y,x))]
[∀x.(evidencetype(x) ∀x(canbe(r) → complianceAccreditation(c,x) ∧ securityLogs(z,x))]
[∀x.(securitylogs(x) ∀x(canbe(r) → applicationLogs(a,x) ∧ userActivityLog(u,x) ∧ eventLog(e,x) ∧ systemLog(s,x) ∧ errorLog (e,x) ∧ otherLog(z,x))]
[∀x.(compliance/accreditation (x)→ evidenceType(x))]
[∀x.(evidencetype(x) ∀x(canbe(r) → complianceAccreditation(c,x) ∧ securityLogs(z,x))]
[∃x.(securityLogs(x) → applicationLog(a,x) ∨ userActivityLog(u,x) ∨ eventLogs(e,x) ∨ systemLog(q,x) ∨errorLogs(e,x) ∨otherLogs(z,x))]
[∃x.(evidenceSource(x) → automatedLog(s,x) ∨ cspPortal(c,x) ∨ whitepaper(w,x) ∨ userExperience(u,x) ∨ auditReport(q,x) ∨ cspAttestation(z,x))]
[∃x(requirement(x) → business(q,x) ∨ basic(r,x) ∨ transparency(y,x) ∨ operational(z,x))]

Figure 5.8: Evidence Ontology

5.4.7 Security Audit

Security audit entails the evaluation of a CSP's infrastructure, policies and operations for determining the effectiveness of systems, processes, and controls, and as well as to the conformance of asset requirements. The objective of this concept is to enable an organization understands the pervasive effect of incidents and other related activities on assets and associated business processes, understand the controls that the CSP uses to manage and control assets, conclude on the effectiveness of CSP controls, recommend the implementation of corrective actions, changes and improvements where needed. Additionally, the exercise performed in this concept are guided by professional audit standard such as ISA 200 (ISA, 2016). The crucial components associated with this concept include:

- *Auditable Requirements:* involves the determination of the range of requirements that are covered during the audit process such as transparency, business or operational requirements.
- *Audit Evidence Collection:* relevant and reasonable evidence is obtained to support an auditor in making judgements and conclusions regarding the requirements and areas of controls under audit. Audit evidence refers to the implicit claims, and assertions, cloud system generated reports and representations supplied by the CSP to manifest how customer requirements are met and how security is achieved. Audit evidence are collected and analysed to draw reasonable audit conclusions based on which audit outcomes are formed. Two primary types of audit evidence can be obtained: security logs and certifications/accreditations. Each evidence type contains a list of other evidence.
- *Audit Report/Findings:* Audit reporting deals with drawing conclusions and developing a report to communicate findings, outcomes, and the actions to be adopted for improving controls or adding controls in response to each requirement that is audited. The audit report is formed based on the provisions of the ISA 700 standard (International Standard on Auditing, 2016). Audit findings are drawn based on defective, acceptable or effective practice. Defective practice implies substantial disparity between audit criteria and CSP evidence; acceptable practice indicates similarity but contains gaps or weaknesses in specific areas; whereas effective practice involves a considerable correlation between audit criteria and evidence.
- *Remedial Actions:* remedial actions are constructive recommendations issued by the auditor when the audit findings substantiate significant improvements in operations and performance of the CSP. Recommendations focus on areas where noncompliance to requirements is noted or significant weaknesses in controls are found. Action plans are mainly directed at resolving the cause of identified problems using corrective, detective or preventive actions.

Table 5.7: Rule-Based Knowledge Representation of Security Audit

[∀x:∃y:(securityAudit(x) → require(r,x) ∧ collectEvidence(y) ∧ auditableRequirement(q) ∃stoenable(s,x) → performAudit(z))]
[∀x::(securityAudit(x) → requires(r,x) ∧ collectEvidence(y) ∧ auditableRequirement(q) ∃s toenable(s,x) → performAudit(z))]
[∀x:(collectEvidence(x) ∨ requires(r,x) ∨ evidenceType(y) ∨ evidenceSource(r) → securityAudit(x))]
[∀x:(evidenceType(x) → canbe(y,x) ∨ securityLogs(s) ∨ complianceAccreditation (r))]
[∀x:(evidenceSource(x) → canbe(y,x) ∨ automatedLogs(a) ∨ whitepaper(w) ∨ webportal(p) ∨ userExperience(u) ∨ cspattestation(c) ∨ auditReport(z))]
[∀x(auditableRequirement(x) ∧ canbe(y,x) → business(b) ∧ basic(r) ∧ transparency(r) ∨ operational(z))]
[∀x(performAudit(x) → has(y,x) ∨ conformanceLevel(r) ∨ auditCriteria(c) ∨ auditReport(z))]
[∀x(auditReport(x) → ∃ycontains(y,x) ∨ remdialActions(r) ∨ auditJudgement(z))]
[∀x(remedialAction(x) → canbe(y,x) ∨ correctiveControls(s) ∧ preventiveControls(y) ∧ detectiveControls(z) ↔ canbe (s,y,z))]
[∀x(auditJudgement(x) → canbe(y,x) ∨ acceptablePractice(r) ∧ defectivePractice(s) ∧ effectivePractice(y) ↔ ¬canbe (r,s,y))]
[∃x(conformanceLevel(x) → canbe(y,x) ∨ veryHigh(v) ∧ high(h) ∧ medium(m) ∧ low(l) ∧ veryLow(y) ∧ nonconformity(z) ↔ ¬canbe (v,h,m,l,y,z))]
[∀x(auditCriteria(x) → completeness(q) ∨ sufficiency(r) ∨ understandability(s) ∨ accuracy(x) ∨ reliability(z)))]

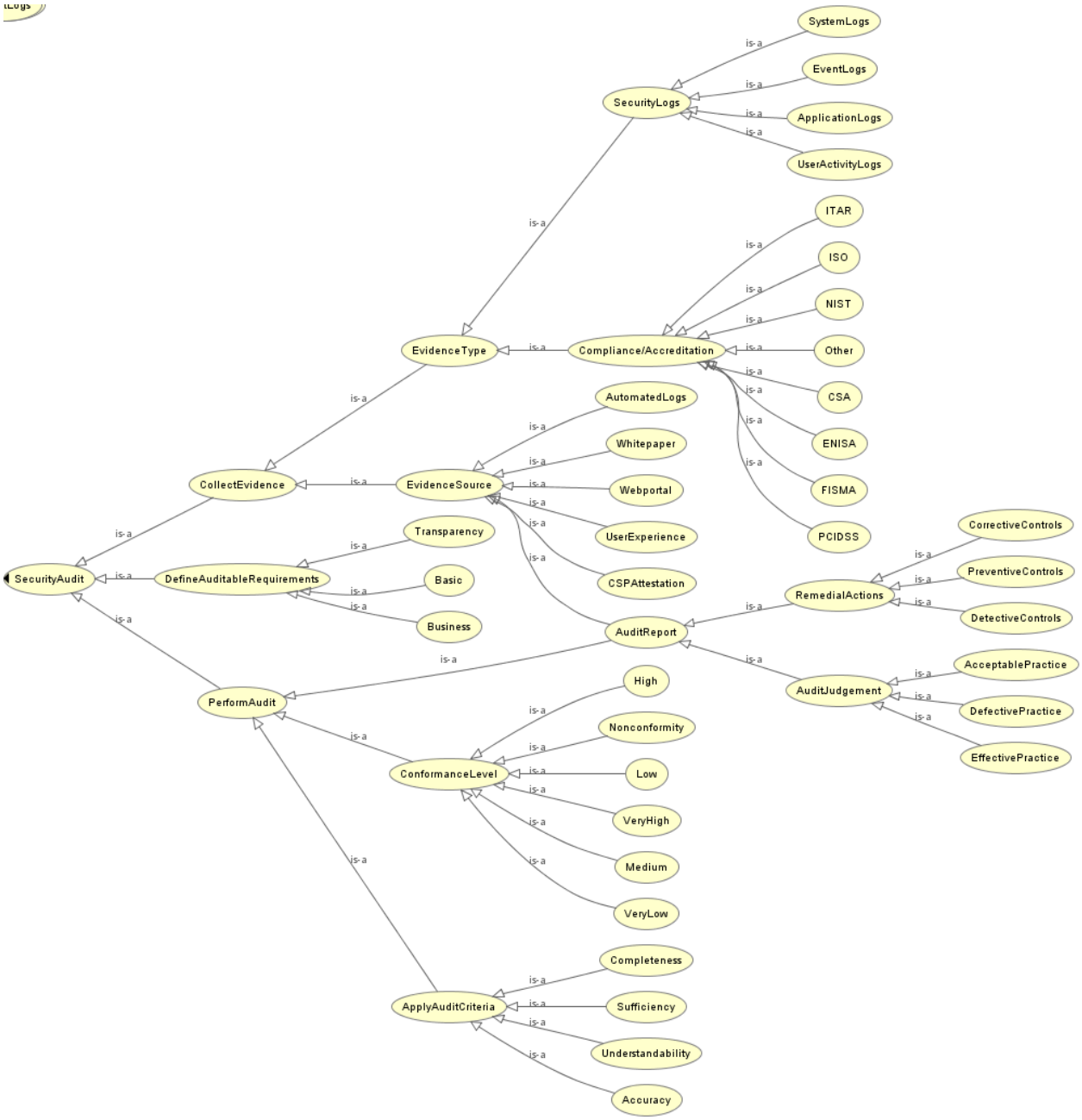

Figure 5.9: Security Audit Ontology

Table 5.7: Rule-Based Knowledge Representation of Security Transparency

[∀x(actor(x) → cambe(y) → internal(q) ∧ (external(z) ¬ canBe(q,z))]
[∃x(actor(x) → internal(q) → perform(r,x) → securityAudit(a) ∨ identifyRisk(r) ∨ assessCSP(s) ∨ collectEvidence(e) ∨ identifyRequirement(z))]
[∀x(asset(x) → canBe(r) ∧ data(d) ∧ software(s) ∧ hardware(q) ∧ process(p) ↔ canBe (r,d,s,q,p))]
[∃x(actor(x) → external(e) → provide(p) → IaaS(I) ∧ PaaS (p) ∧ IaaS (y) ↔ provide(I,p,y))]
[∀x(asset(x) → ∃ycanHave(y,x) ∧ securitygoals(s) ∨ requirements(r) ∨ criticality(c))]
[∀x(securityGoals(x) → ∃ycanHave(y,x) ∧ confidentiality(c) ∧ integrity(t) ∧ availability(a) ∧ accountability(r) ∧ conformance(n) ∧ canBe(c,t,a,r,n))]
[∀x(criticality(x) → canBe(y,x) ∧ high(h) ∧ medium(t) ∧ low(z) ¬canBe(h,t,z))]
[∀x(risk(x) → obstructs(y,x) ∧ securityGoals(q) ∧ assets(z) ↔ obstructs(q,z))]
[∀x(controls(x) ∧ ∃ymitigate(y,x) → risks(r))]
[∀x(requirement(x) → ∃yinclude(q,x) ∧ transparency(t) ∧ basic(b) ∧ business(s) ∧ operational(o) ∧ include(t,b,s,o) → protect(r.x) assets(z))]
[∃x(actor(x) → internal(s) ∧ impose(s,x) ∧ ∃yrequirement(r))]
[∀x (actor(x) → external(s) ∧ ∀yconform(c,x) → requirement(r))]
[∀x(actor(x) → externall(e) ∧ ∃yprovide(p,x) ∧ evidence(y) → satisfy(s.x) assessCSP(r))]
[∀x(actor(x) → externall(e) ∧ ∃yprovide(p,x) ∧ evidence(y) → satisfy(s.x) requirement(r))]
[∃x(actor(x) → internal(s) ∧ asses(c,x) ∧ ∃CSP(r,x) ∧ beforeMigration(q) ∨ securityAudit(z))]
[∃x(actor(x) → external(s) ∧ provides(r,x) ∧ ∃evidence(e) → support(y,x) assessCSP(q) ∨ securityAudit(z))]
[∃x(evidence(x) → canBe(c.x) ∧ beforeMigration(q) ∧ securityAaudit(z))]
[∀x(actor(x) → externall(e) ∧ ∃yprovide(p,x) ∧ evidence(y) → satisfy(s.x) assessCSP(r))]
[∀x(actor(x) → externall(e) ∧ ∃yprovide(p,x) ∧ evidence(y) → satisfy(s.x) performAudit(r))]
[∀x∀y(evidence(x,securityLog) ∧ evidence(y, complianceAccreditation) → evidence(x = y))]
[∀x(evidence(x)→ beforeMigration(y) ¬ support(s,x) assessCSP(z))]
[∀x(evidence(x)→ securityAudit(y) ∃ysupport(y,x) performAudit(z))]
[∀x(assessCSP(x)→ requires(r,x) assessmentCriteria(y) ∨ principleOfTransparency(p) → ∃!select(s) ↔ CSP(q,x))]
[∀x∀y∀z(assessCSP(x)→ canHave(c,x) ∃!assessmentResult(r,x) → opaque(y) ∧ explicit(z) ¬ canHave(c,r))]
[∀x(securityAudit(x) → canHave(c,x) ∃performAudit(y) → auditReport(s) ∨ conformanceLevel(c) ∨applyAuditCriteria (z))]
[∀x∃!z(CSP(x) → ∃!canHave(c,x) ↔ conformanceLevel(z,x))]
[∃x(actor (x) → internal(a) ∃canSpecify(c,x) remedialActions(z))]
[∃x(CSP(x) → mustImplement(c,x) ∃remedialActions(z))]
[∀x(CSP(x) ∨ auditJudgement(r, AcceptablePractice) ∨ auditJudgement(n, effectivePractice) → transparent (z))]

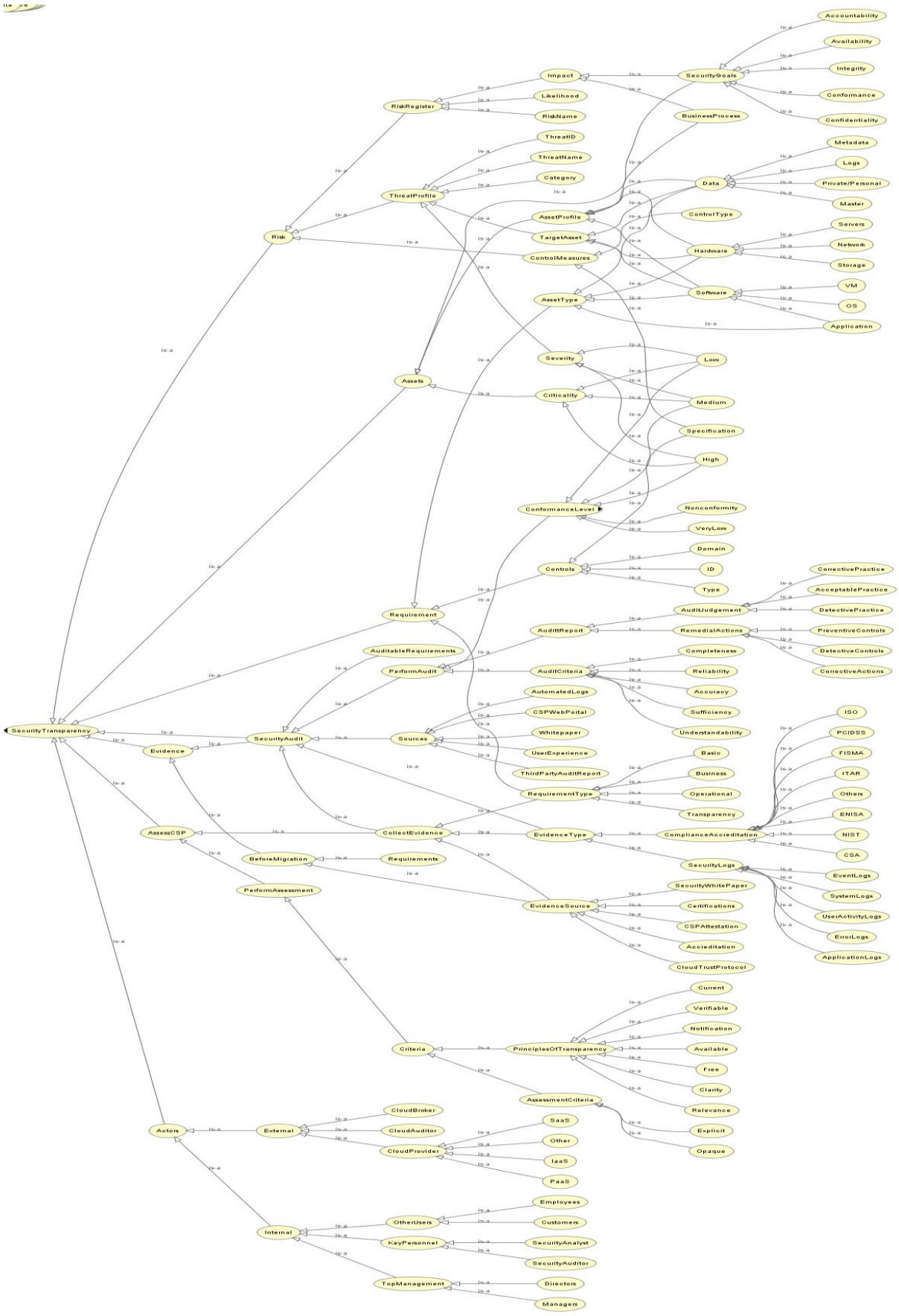

Figure 5.10. Ontology for Overall Security Transparency Concepts

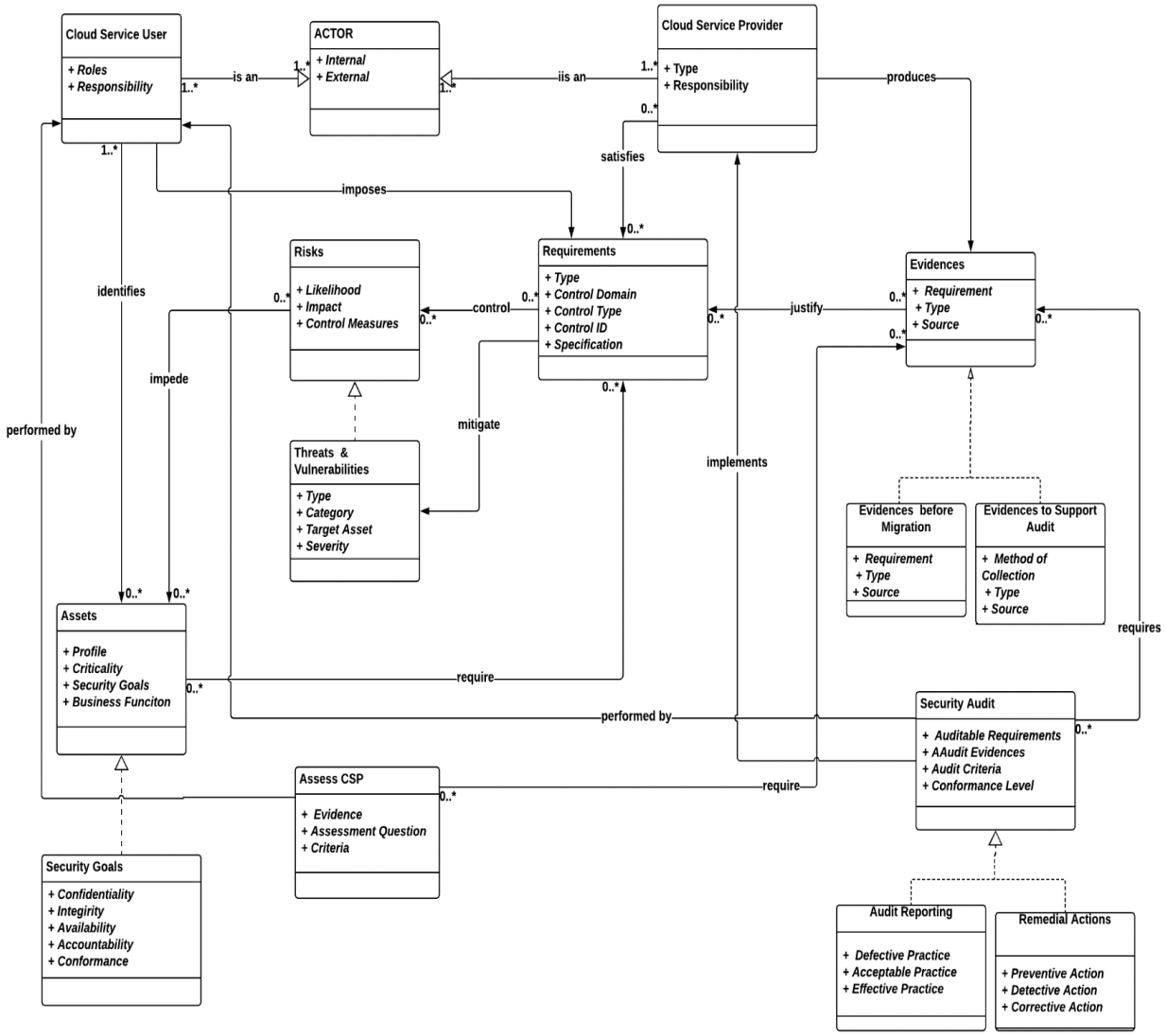

Figure 5.11. A meta-model for security transparency at an organizational level.

The meta-model in Figure 5.11 shows an overall view of the concepts at the organizational level and their relationships. An actor could be an organization that is interested in cloud services offered by a CSP. At the preliminary stages of cloud adoption, the organization performs an appraisal of the stakeholders, both internal and external, that will be actively involved, or whose interest should be taken into account in the transition to a cloud environment. The identification of actors is essential not only for determining the roles played by actors but also for the implementation of the framework's process. An organization owns a wide range of assets that require several security goals for supporting the business process. As a result, assets that are critical to operations are comprehensively profiled to include the security goal every asset must achieve, the business process supported by assets, and importantly, the criticality of each asset to the organization. Also, assets are usually connected to one or many forms of risks, especially as a result of adopting cloud services. An organization systematically

identifies the risks that could potentially affect assets, associated threats, including a prioritized estimation of the likelihood, impact of security risk scenarios and the security measures that can be applied to controlling to risks. Diversely, CSPs, implement necessary technical and non-technical controls for safeguarding customers' assets, as well as transparency mechanisms for divulging information to customers regarding operational practices. In addition, the CSP adopts proactive or reactive transparency mechanisms to generate evidence in various forms to support potential customers' access to information regarding CSP services or provide existing customers with essential data, system or application report that can assist customers in performing on-going verifications to conformance of expectations. An organization considers CSP evidence and specifies specific requirements that must be met. Therefore, requirements are specified from different viewpoints such as transparency, basic, operational and business requirements. The requirements specified become the prioritized areas that the organization continuously evaluate after migration to the cloud. Therefore, the evidence must be provided by the CSP regarding how such requirements are being satisfied. This is where monitoring plays a significant role and the primary purpose monitoring is to track the status of the requirements, user and system activities and generate many forms of reports that are shared with the organization. The reports subsequently serve as evidence that is subject to vetting using a security audit. The security audit is aimed at producing a clear audit report based on findings from evidence to establish how well requirements are met and how controls are operated.

5.5 Technical Level

This is the final level of abstraction in the framework that is mainly influenced by the organizational level. As stated earlier, the organizational level provides essential concepts that support the understanding of how security transparency can be achieved, including the relevant methodology for attaining security transparency. Thus, the primary focus of the technical level is to describe the technical means for realising transparency. This consistent flow further illustrates the connection and interdependence between the three levels of abstraction that can be viewed from a conceptual view, the organizational level down to the technical level. However, before we dwell into that, it is imperative to briefly highlight some essential conventional initiatives or mechanisms that can be utilised to achieve security transparency at the technical.

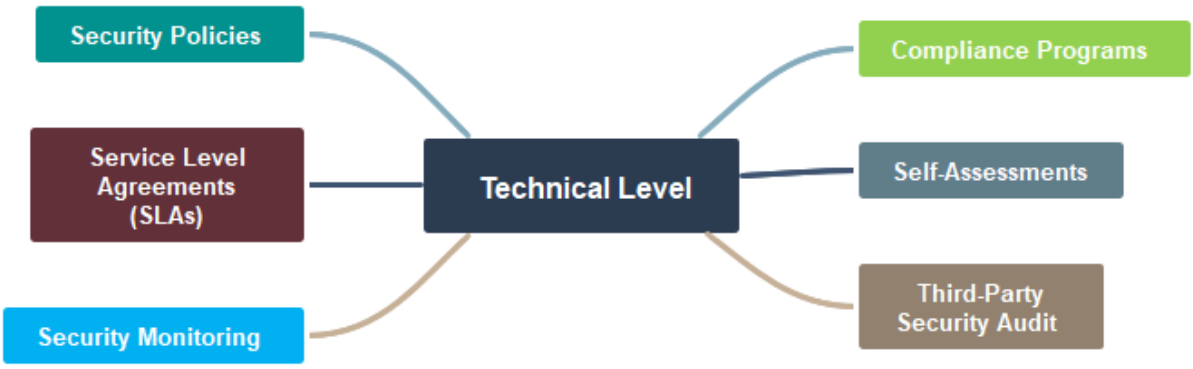

Figure 5.11: Means of Security Transparency at Technical Level

5.5.1 Compliance Programs

CSPs increasingly use compliance programs as mechanisms for demonstrating transparency through conformity with many traditional standards that predominantly focus on certifying the composition and management of security practices in their environments. Consequently, CSPs earmark a significant monetary budget for ensuring security and spend a sizeable amount of resources and time into compliance with security standards such as ISO 27001/27002, Payment Card Industry Data Security Standards (PCI DSS), and other relevant standards.

5.5.2 Self-assessments

CSPs have realised the obligation to provide satisfactory transparency of their services to organisations. They often conduct a discretional self-assessment of their services by employing control objectives specified in frameworks that document and certify best security practice within their environment to provide transparency to customers. Self-assessments are usually free and open to all CSPs. One such framework is CSA STAR Certification that embarks on a three-levelled certification scheme to certify CSP's compliance with its set of security guidance and control objectives.

5.5.3 Security Policies

CSPs enforce security transparency policies that make them committed to making information available to the public on demand. CSPs consider access to information a key component of active participation of all organisations. Transparency policies are often enforced through an Information Disclosure Policy, which is guided by the underlying principles of accountability and openness concerning operational programmes and customer-related aspects.

5.5.4 Service Level Agreements (SLAs)

Another important technique for ensuring adequate disclosure of information involves the use of SLA. The SLA is a binding contract between the CSP and their customers, which specifies customer

requirements and the CSP commitment to fulfilling them. It clearly describes the security responsibilities and liabilities between the two parties, states the service performance and delivery, problem management, legal compliance, *etc*.

5.5.5 Security Monitoring

Security monitoring involves processes enabled by the CSP for the systematic collection and analysis of events of interest relating to customer data to respond to security incidents of interest, as well as providing a great structure to predict future security-related issues. A well-structured cloud security monitoring supports timely dissemination of security occurrences to interested actors for a decision on the appropriate course of action that ought to be taken. Security monitoring also plays an essential role of enhancing accountability and mutual trust using making CSP accountable for security violations that emerge as a result of deficient controls in their services, helps customers detect a breach of SLA contracts, and helps in the gathering of evidence to validate the security claims of a CSP. On the part of a CSP, it empowers the capturing of the current security state of cloud systems; deviations from expectations and the monitoring of clients' activities to ensure malicious use of resources are prevented.

5.5.6 Third-Party Audit

This is another type of transparency mechanism that materialises in the form of a systematic and objective examination of CSP premises, which is mostly initiated by an independent auditor appointed to appraise the CSP environment physically.

5.6 The Adoption of Audit as a technique for Security Transparency

The research adopts security audit as the technique for achieving security transparency at the technical level. A specially built Security Transparency Audit Tool (STAT) is designed to serve as a platform on which an organisation can probe the activities of a CSP by seeking information about specific requirements and receiving evidence about the extent to which CSP fulfils the requirements. STAT is designed to enable organisations to leverage a dedicated security audit checklist that focuses on the many aspects of organisation's requirements to probe CSP and receive evidence that is analysed to form an audit judgement regarding CSP's conformance to requirements.

This process is enabled through a query-response approach that is initiated and controlled by the organisation where the CSP responds to a request by supplying relevant evidence. STAT also enables customers to receive alerts when specific requirements are met using a communication protocol for message-oriented middleware based on XML (extensible Mark-up Language). The tool additionally provides an assessment facility that can be used to assess.

It is important to emphasize that STAT mainly proposes a unified, standardized API to present measurement results related to CSP conformance. As such, the audit tool does not cover the actual monitoring infrastructure and related technologies that are used to gather, store and analyse events to produce these measurement results.

CHAPTER SIX

Process for Security Transparency

6.1 Introduction

This chapter presents an overview of the underlying process involved in the cloud security transparency framework. Primarily, the process aims to introduce different phases of activities that organisations can follow for understanding and strengthening cloud transparency by looking at essential considerations such as identifying roles, assessing risks, and evaluating CSP controls. The process will also help organisations to build a cloud migration profile from scratch to the end, meaning that they will be able to complete the transition to the cloud and also have the ability to validate whether expectations are being met by the CSP continuously. Therefore, the principal beneficiaries of the framework and its process are organisations (including public or private establishments) who aspire to or have the responsibility for security transparency and data protection. Hence, it is essential to emphasize that the framework does not focus on individual cloud users who usually do not have as much obligation towards security transparency, diverse requirements and responsibilities as organisations.

A crucial aspect of the process is that it provides methodical activities for developing an efficient cloud migration approach that is mainly security transparency-oriented, and which provide a roadmap for organisations to achieve security transparency. The core of the process includes several diverse activities and steps to help guide key decision points about organizational context, cloud transition activities, potential risks, control measures, as well as the verification of CSP compliance to security controls. It helps in identifying and interlinking cloud migration components for ensuring efficiency, effectiveness and consistency within different areas.

Another essential feature of the process is that most of the activities are formed by considering a variety of leading industry best practices, frameworks, guidelines and standards that are generally applicable to all organisations regardless so their size or the sector in which they operate. This implies that the process is all-encompassing in nature, and not tailored to a specific organisation type or solution, but built upon high-level considerations to ensure important cloud adoption issues are not overlooked.

6.2 Cloud Security Transparency Framework Process: A Unified Approach

The process for the security transparency framework is simply a unified approach that leverages existing industry standards to assist organisations in attaining security transparency by ensuring that every step and activity is performed according to generally accepted security principle. Sections of renowned industry standards, guidelines, frameworks and models were applied across different activities within the process by looking at specific features within the standards and where they can be applied in the process. For example, CIS CSC and ENISA are used for identifying risk control measures. This is because CIS CSC provides 20 controls categorized into three prioritized and defence-in-depth best practices that are implementable to mitigate attacks against systems and networks. Some of these

controls are relevant to cloud security transparency, while others are less relevant. Further, ENISA provides 27 baseline security controls that are more CSP-oriented and focuses on control measures that protect cloud computing systems against operational risks. As a result, a parallel matching is performed for identifying semantic equivalence between controls in CSC CIS and ENISA. Besides, Microsoft has proposed a structured approach for analyzing the security of systems and application namely: DREAD and STRIDE models. Such models enable the identification, classification, rating, comparison and prioritization of security risks associated with systems and applications, and these two relevant models have been adopted for threat analysis. OWASP methodology is also used for determining the impact of risks because it estimates risks from business process and technical perspectives, and it is highly adaptable and applicable to most organizations of all sizes. In identifying relevant risks, risk sources from ENISA and OWASP are considered mainly because the latter maintains a regularly-updated list of most pressing cloud security concerns, and the former provides a list of 35 risks that fall under categories such as technical, organizational, legal and non-cloud specific. Also, in the course of specifying requirements, CSA STAR is adopted because it provides sixteen essential security principles that serve as a guide to CSPs and also provides organisations with the structure to achieve asset security in the cloud-tailored environment. In the audit activity, ISAE 3402 and ISO 19011:2018 is used mainly because it sets forth internationally accepted guidance on conducting and managing audit program that applies to all organisations that need to conduct security audits. An overview of the different standards, frameworks, and models and the features or aspects derived from them is provided in figure 6.1.

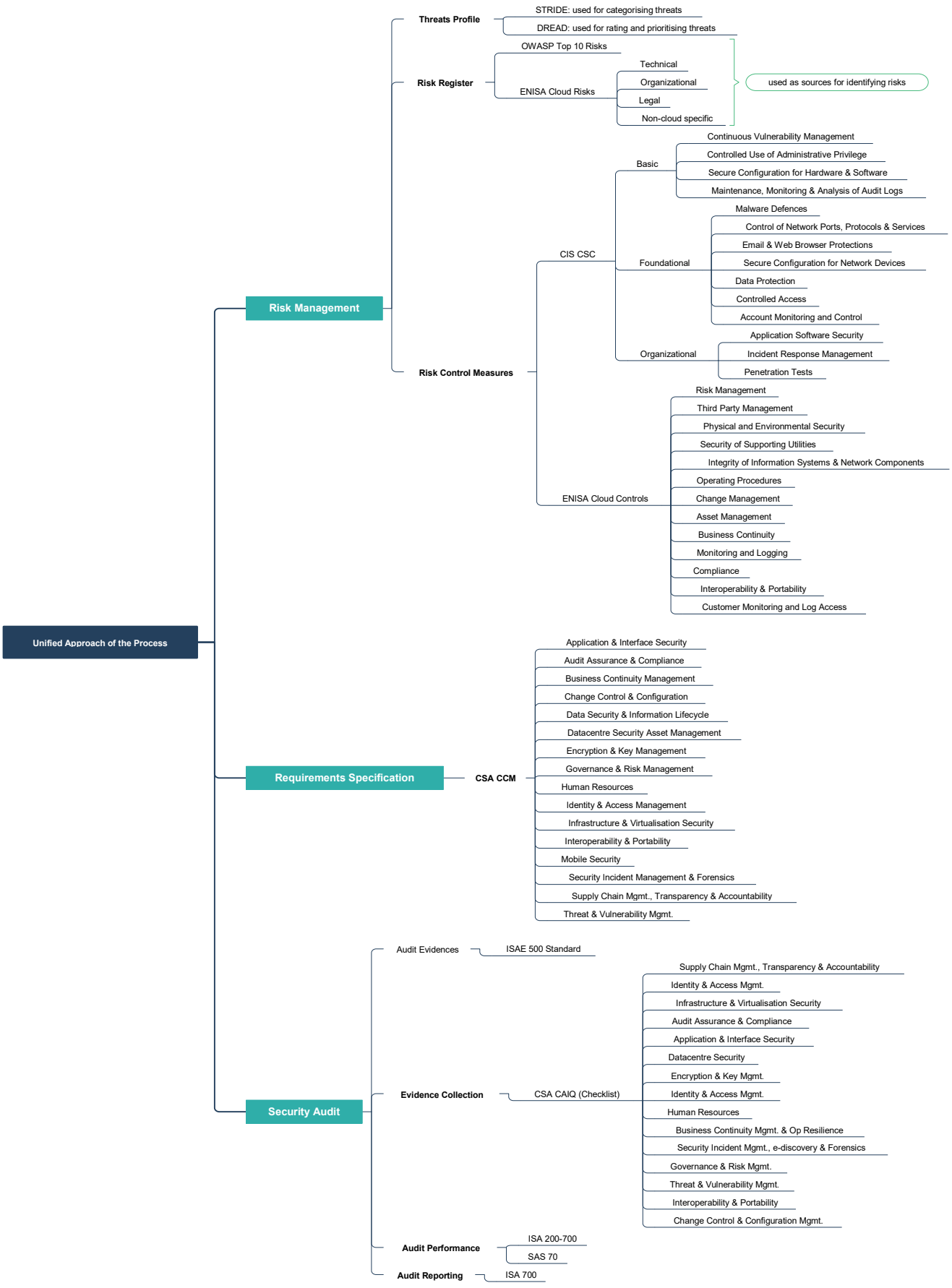

Figure 6.1: A Unified Approach to Cloud Security Transparency

6.3 Security Transparency Framework Process

From the perspective of the research, a process is considered as a structured set of activities that are executed towards accomplishing security transparency. A process establishes a strong relationship between multiple steps for effective delivery of expected outcome. An activity deals with interdependently linked tasks that receive and convert one or more input into an output artefact (Knight and Burn, 2005, Beer, 1984). The process provides a means of contextualising an organisation, profiling risks, eliciting, and examining security requirements. The intent is to integrate distinct considerations into a complete exercise at the early stages of cloud computing adoption. The process manifests efficiency and adequacy for analysing the security aspects of cloud adoption and has the potential for enhancing trust and assurance in cloud services.

The process also provides an overview of essential phases that an organisation has to take into account when adopting cloud solutions with security transparency in mind. For simplification purposes, the process is decomposed into 3 phases, and each phase contains many activities and steps that provide a lower level of detail, as outlined in Table 6.1. The division of the process is imperative in creating a comprehensive set of related activities that allow organisations to identify and achieve deliverables for security transparency. Phase one (context analysis) focuses on the scope of the organisation for gaining a comprehensive understanding of supported assets, their functions and essential security requirements. Phase two provides a security transparency-oriented decision support for assessing CSP transparency level and selection of cloud offerings. It is important to emphasise that Phase Two of the process is optional and is mainly intended for organisations that are at the early stages of cloud adoption and pondering on the selection of a suitable CSP that is capable of supporting security transparency. In other words, Phase Two is developed to facilitate the selection of commercially available CSPs based on the provider's support for security transparency. Various cloud offerings must be compared and assessed based on security transparency capabilities before cloud adoption. Therefore, the step could be inessential for organisations that have already evaluated CSP offerings. Lastly, phase 3 deals with the application of a systematic audit process for determining CSP conformance to security requirements prescribed by an organisation. Each activity specifies the steps that need to be followed, and each step identifies the needful inputs, participating actors and final output.

Primarily, the output of each activity serves as the input to the next activity that follows it. The efficacy of the process is mostly achieved when conducted with the support of primary and a team of security auditors and experts delegated by an organisation to oversee the cloud migration project. Hence, an organisation must delegate suitable actors to participate in and supervise the implementation of the process.

Table 6.1: Security Transparency Framework Process

Phase	Activity	Steps	Input	Technique	Performed by	Output
Phase One: Context Analysis	**Activity 1:** Stakeholder Analysis	Identify Actors	Grouping of actors according to internal and external. Internal actors represent the respective roles and responsibilities of personnel/departments within an organisation. External actors include stakeholders that are involved in the delivery of cloud services.	Examining job profile, duties, roles and responsibilities of actors	Cloud user	A defined list of actors and their roles
	Activity 2: Define Organizational Context	Assets Profiling	An overview and list of organizational assets detailing assets core functionalities and subcomponents.	Review of asset inventory, audit reports, security policy, interviewing cloud users and physical observation of assets	Security Analyst and Cloud Users	Description of assets, functions, and subcomponents owners, criticality and required level of protection
		Identify the security goals of assets	Existing asset profile	Combination of asset control principles and the organisation's security policies	Security Analyst and Cloud Users	Enumeration of security goals and principles that each asset must achieve for sustained operations of the organisation
		Determine asset criticality	Agreed upon asset profile and goals.	Employing asset criticality ranking using impact value and weight score to determine criticality level	Security analyst	Consistent and unambiguous classification of assets according to the criticality level to the organisation's processes and functions.
		Identify business process	Business operational structure and type of services provided	Review of existing processes, facilitated workshops and interviews to collect information	Business Analyst and Security Analyst	A description and alignment of business processes to organizational goals and assets.
	Activity 3: Risk Management	Determine Threat Profile	Organizational assets and goals, list of threats and vulnerabilities provided by ENISA and CSA	Employing Microsoft's STRIDE and DREAD models for threat analysis.	Security Analyst	A comprehensive threat profile detailing potential threats to assets categorisation and determination of threats according to STRIDE and DREAD models,
		Create a Risk Register	A collection of security risks from OWASP, CSA and ENISA that are associated with the threats identified, including implementation controls from CSC CIS.	Application of OWASP risk methodology that estimates risks from business process and technical perspectives estimates risks likelihood, risk impact, and control measures	Security Analyst	A detailed risk register highlighting risks, impact, likelihood, rating and recommended controls

	Activity 4: Requirements Specification	Specify security transparency and other requirements	Consideration of security transparency, business process, operational and basic security requirements according to the provisions of CSA CCM	The use of recommended and predefined categorisation of requirements that can be specifically tailored to an organisation's needs.	Security Analyst	Requirements specification Matrix prioritising must be present in cloud controls to provide a secure environment and security transparency
Phase Two (Optional): CSP Security Assessment and Selection	**Activity 5:** Assess CSPs	Collect CSP Information before Migration	Information from multiple CSPs based on certain types, and specifically, how they can support the attainment of transparency, business, basic and operational requirements.	A detailed search of CSP web portals, security whitepapers, CSP attestation, audit report, industry accreditation and certification.	Security Analyst	Formal and explicit declarations from CSPs affirming the implementation of security control procedures and processes according to the organisation's requirements.
		Assess CSP Security Transparency	Declaration and attestation from CSPs on security controls, procedures and processes	Assessment questions and criteria that enable the ranking of CSP capability of delivering security transparency	Security Analyst	Determining the type of security transparency provided by CSPs based on the opaque or explicit criterion
Phase Three: Security Audit and Reporting	**Activity 6:** Security Audit	Define Security Requirements to be Audited	The list of security requirements identified in activity 4.	Facilitated a preliminary survey of the final list of security requirements	Security Auditor	The depth and areas of controls and requirements that will be covered in the audit
		Collect Evidence for the requirements to be audited	The requirements and areas of CSP controls to be examined and assessed	A manual technique involving a questionnaire derived from CSA's Consensus Assessments Initiative Questionnaire (CAIQ). An automated technique for analysing evidence.	Security Auditor	The collected set of documentary evidence to support the drawing of the audit opinion.
		Perform Security Audit	Documentary evidence provided by the CSP and logs and reports generated by automated monitoring tools	A metric and scorecard for analysing, examining and comparing evidence against a criterion for quality evidence provided by SAS 70	Security Auditor	Determining the level of CSP conformity to security requirements and ensuring adequate controls in their environment.
		Generate Audit Report	The result of findings based on examining and analysing CSP evidence	Manual and automated documentation of findings	Security Auditor	Provide actors with unbiased and reasonable opinion on the adequacy, effectiveness and conformity of CSP relating to controls defined in the audited requirements.

6.3.1Activity 1: Stakeholder Analysis

According to Goodpaster (Goodpaster, 1991), a stakeholder is any entity with a conceivable interest or stake in an activity. A stakeholder can be an individual, group of individuals or an institution affected by or who can influence the impact of an activity. The Stakeholder analysis involves the identification of major actors, an assessment of goals, and how they impact the cloud adoption and its viability. Stakeholders are actors such as top management, administrators, etc. who are directly or indirectly involved in influencing the success of the organization and its processes. The relevance of this activity is to obtain a comprehensive picture of actors and their roles in meeting requirements. This becomes important in identifying potential conflict of interests and other issues such as the actors responsible for the design, development, and maintenance of cloud-bound assets.

6.3.1.1 Step 1.1: Identify Actors

Actors are the entities that will contribute to the cloud migration-related decisions. Actors interact with the cloud system or relationship with one another through actions such as providing technical and nontechnical support or services to the organisation. The nature of interactions between actors needs to be clearly interpreted, balanced, reconciled and managed accordingly. Actors are identified based on their input for ensuring the success and delivery of operations for the organisation, as well as those that are ultimately affected by the transition of backend organizational asset to the cloud such as employees of an organisation. To optimally carry out an organisation's transition to the cloud, an organisation must identify who the key actors are. In this case, actors can be identified according to internal and external actors. Internal actors include the organisation itself and skilled personnel who play different roles within an organisation such as a security analyst, risk manager etc. External actors mainly include the CSP and other third-party that provide some form of services to the CSP. Table 6.2 provides a listing of actors and their roles. However, the listing of actors varies and will be determined in every organisation according to its volume of activities and resources.

Table 6.2 Actors, and Roles

Internal (Organisation)		**External (CSP)**	
Actor	**Role**	**Actor**	**Role**
Cloud user (CU)	Represent the organisation that owns information and assets for whom cloud services are created to support and who maintains a business relationship with a CSP. Cloud users represent the functional areas within an organisation, such as the business department, IT departments.	CSP	Represents an organisation or an entity that is responsible for making a service available to an organisation. CSP builds and manages the requested platform or infrastructure service, and ensure the security protection, privacy and privacy of an organisation's assets, and provides the fulfilment of agreed-upon transparency and security requirements of an organisation.
Security Analyst (SA)	Responsible for identifying cyber threats and establishing plans and controls to protect assets. Also responsible for performing vulnerability testing, risk analysis and security assessment activities.	Cloud service auditor	An independent third-party that conducts assessments of cloud services, information system operations, and performance and security implementations within cloud services. Cloud auditor also

			performs an unbiased evaluation of cloud security controls to determine the extent to which controls are implemented correctly, operating as required, and produced desired outcomes as per the requirements of an organisation.
Internal Security Auditor (Sec Aud.)	Probes the safety and effectiveness of security controls and related security components of assets. Also, plans, execute and lead security audit, including evaluating the efficiency, effectiveness and compliance of business processes with organisation requirements, including generating a written report on audit findings.	Cloud service broker	Represents a third-party business or individual that acts as an intermediary between an organisation and the CSP. An organisation may decide to request cloud services from a broker instead of directly contacting a CSP, in which case the cloud broker manages the use, performance and delivery of cloud services, as well as negotiating the relationship between an organisation and the CSP.

6.3.2 Activity 2: Define Organizational Context:

Each organisation is unique and usually operates within a defined scope and available resources. To successfully execute the process and achieve a sound cloud adoption, it is essential to perceive each organization from within its operational context. Organizational context tends to establish a better understanding of the current state of the organisation. Tailoring the cloud migration to organizational context helps an organisation to ensure essential cloud migration factors are considered, and in general, increase the likelihood of success. It is the second activity of the process because it is pivotal to relate security transparency from operational perspectives succinctly. Therefore, the chief information security officer (security analyst) who has significant familiarity with the organisation's line of business and the need behind the adoption of cloud services to examine the essence of the organisation's use of assets while considering the laws and regulations binding on the organisation that may limit the use of information in the context of cloud services, critical nature of asset for the organisation to function, and the level of protection for the assets. The primary output artefacts of this business process details involving four steps:

6.3.2.1 Step 1: Assets Profiling

The basis of this step is to profile assets in terms of their boundary, components, and assigning weight to the assets based on assets important to the organization. Assets are specific units such as a database, application or program that support the delivery and usage of services offered by an organization. To create asset profiles, a Security Analyst is involved in identifying assets by considering assets' core functions, alongside other subcomponents that are essential to achieving and maintaining crucial functions. Important asset information can be gathered by reviewing background materials, including independent audit/analytical reports, interviewing cloud users, and physical observation of organizational assets. Also, asset specification and management documentation provide important details about the organizational asset.

6.3.2.2 Step 2: Identify Security Goals of Assets

Security goals are specific attributes, which are also referred to as security principles; they describe assets' expected conformance to secure behaviour. Identifying security goals is an essential consideration to allow an organisation to determine what critical tenets of security must be ensured each asset during storage, processing or transmission, by authorised systems, applications or individuals. Also, security goals are used in determining the impact that may result from accessing assets in an unauthorised manner for use, disclosure, interruption, change, etc. Therefore, the Security Analyst considers a set of security goals that each asset aims to achieve. By doing this, the consequential impact that may ensure the compromise of the security goals and the level of protection needed can be easily determined. We have defined a set of asset security goals every asset must aim to achieve such as:

- **Confidentiality**: Assets must be protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that only those with predefined rights and privileges to access an asset can do so. A breach to confidentiality is the unauthorized access, disclosure or manipulation of the asset.
- **Integrity:** Assets must be guarded against unauthorized modification and alteration. The integrity of asset is compromised when it is exposed to illegitimate modification, alteration, damage, destruction or disruption of its authentic state.
- **Availability:** Assets must be accessed only by authorized users or systems without interference or obstruction. Assets must be available when requested, and if interrupted, the asset must recover and continue secure operations without adverse side effects. The loss of availability is the disruption of access or use of an asset
- **Accountability:** Requires the tractability of actions, attack or incidents that occur to an asset to the responsible system or actor. It must be ensured that an authorized actor or an attacker who acts cannot deny involvement.
- **Conformance:** Assets must operate as intended without variation to expected behaviour, functions and regulatory requirements. The asset must be secured from vulnerabilities that can be exploited to cause unwanted behaviour. Any breach or deviation from specified behaviour constitutes nonconformance.

6.3.2.3 Step 3: Determine Asset Criticality

It is highly imperative to determine the criticality of all assets that are migrated to the cloud by performing a criticality assessment. The criticality assessment provides the foundation on which an organisation can identify control measures and requirements. In other words, the assessment aims at assessing the criticality for each asset. Asset criticality is imperative for prioritising and developing actions that will reduce risks to the asset, improve asset reliability, as well as defining cloud strategy in terms of the suitable cloud deployment and service model that should be adopted. In doing so, the primary security goals of an asset are assessed and the consequences of loss of the security goal

established using two factors as criteria: Impact on Business Process (IBP) and Impact on Goals (IoG). Therefore, the criticality assessment of all assets is carried out by a team of experts, with good expertise of knowledge of the organisation's business process and assets.

To ensure validity, consistency and support stakeholders in assessing asset criticality, a decision support system using Fuzzy Set Theory is created. A fuzzy set theory provides a way of absorbing the uncertainty inherent to phenomena whose information is unclear and uses a strict mathematical framework to ensure precision and accuracy, as well as the flexibility to deal with both quantitative and qualitative variables (Zimmermann, 2011).

6.3.2.3.1 Fuzzy Asset Criticality System

A Fuzzy Asset Criticality System (FACS) is developed (Figure 6.2) which uses IoG and IBP as two fuzzy inputs for assessing the level of criticality (LoC) of individual assets. FACS comprises two fuzzy events that serve as the system inputs, i.e. IoG and IBP, one inference engine with 25 IF-THEN rules based on Mamdani (Cordón, 2011) and Sugeno (Sugeno, 1993) approaches, with one crisp output after the de-fuzzification process.

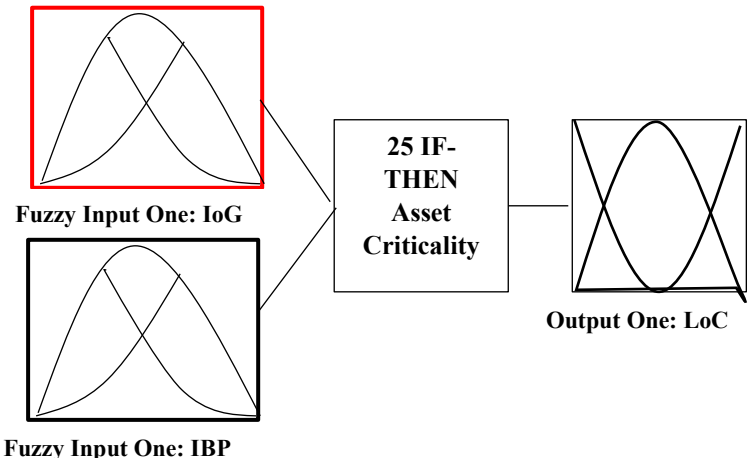

Figure 6.2: Fuzzy Asset Criticality System

6.3.2.3.2 Fuzzy Inputs and Outputs

IoG and IBP are used as two fuzzy inputs, assigned to five fuzzy labels respectively as shown in Table 6.3 and 6.4. The five labels for IoG are VH, HG, MD, LW, and VL, while the five labels for IBP include: NI, LI, MI, SI, VI, respectively. For comparison reasons, corresponding scores are illustrated in the left-hand column of the tables to show how they are used in FACS.

Furthermore, the corresponding membership functions for the fuzzy set are also defined. A triangular membership implies membership function that is used for IoG and which gives numerical interpretation to each fuzzy set. On the other hand, membership functions for IBP are represented to provide a numerical connotation for each fuzzy set for IBP.

Table 6.3: Fuzzy Labels for IoG

Score	Impact on Goals (IoG)	Fuzzy Labels
0	Very High	VH
1	High	HG
2	Medium	MD
3	Low	LW
4	Very Low	VL

Table 6.4: Fuzzy Labels for IBP

Score	Impact on Business Process (IBP)	Fuzzy Labels
0	No impact on business process	NI
1	Low impact on business process	LI
2	Moderate impact on business process	MI
3	Serious impact on business process	SI
4	Catastrophic impact on business	CI

Table 6.5: Fuzzy Labels for Levels of Criticality (LoC)

Crisp Score	Fuzzy Score	Level of Criticality	Fuzzy Labels
0	≤ 0.5	Low	L
1	$0.5 < \leq 1.5$	Medium	M
2	$1.5 < \leq 2.5$	High	H
3	$2.5 <$	Very High	H

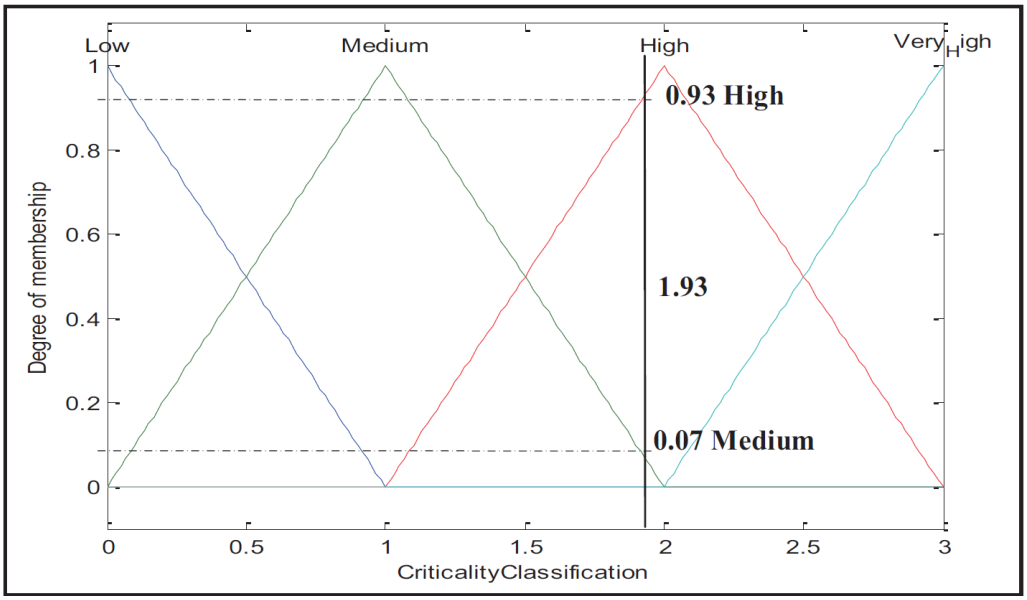

Figure 6.2: Membership Functions using Mandani Approach

6.3.2.3.3 De-fuzzification and Crisp Output

The IF-Then rules are presented in a matrix form (as shown in Table 6.6), which uses the labels of one input in rows and the label of another input variable in columns. Cells in the matrix contain output labels that indicate the possible output resulting from a specific combination of rows and columns. Therefore, using IoG and IBP as inputs, LoC is generated as output, as shown in Table 6.6.

Table 6.6: Matrix for Asset Criticality Classifications

IoG / IBP	VH	HG	MD	LW	VL
NI	L	L	L	M	H
LI	L	L	L	M	H
MI	L	L	M	M	H
SI	L	M	M	H	H
VI	L	M	H	H	(VH)

The LoC for each asset (according to Very High, High, Medium, Low) is mainly obtained using minimum-maximum inference, which considers the minimum of the antecedents of the maximum for aggregation and defuzzification. Hence, the LoC for each asset falls under one of the four categories from low to very high as defined in Table 6.5

6.3.2.4 Step 4: Identify Business Process

A business process is a set of structured and measured activities designed to produce specific outputs for an organization. The business process aims to identify the operating process of an organization, including a review of existing processes and aligning them with assets to discover how cloud services can support operations. Our method of the business process consists of organizing facilitated workshops and interviews with strategic management to identify and collect information relating to functional business processes of the organization. The business processes identified are used to create a link with the usage of assets.

Table 6.6 Asset Inventory

Asset ID	Asset Name	Asset Description	Business Process	Asset Goals	Asset Criticality			Required Protection		
					Low	Medium	High	Low	Medium	High

6.3.3 Activity 3: Risk Management

Risk management activity focuses on identifying and measuring risks related to the assets, as well as identifying essential controls for mitigating the risks. The Security Analyst performs this activity. Based on the assets identified in the previous task, all possible threats that could negatively impact the assets are profiled in a register. However, effective identification and control of threats require an understanding of threat sources, adversary behaviour, capability and intent (Workman et al., 2008). Only through an understanding of threat landscape can an organization have enough knowledge about the nature of threats they face and the control measures to implement. In other words, a holistic understanding of threats enables a more effective prioritization of control actions and decision making. This is possible when categorization is used to allow an organization to understand and create a threat profile expansively. Because of these considerations, the thesis has created two steps for risk management involving: (i) the determination of threat profile; and (ii) creation of a risk register.

6.3.3.1 Step 1: Determine Threats Profile

Determining the threat profile is vital because it allows the identification and understanding of threat characteristics. The determination of threats requires a structured representation of threat information that is expressive and all-encompassing due to the dynamicity of the cloud environment. A Security Analyst must use a sound approach that enables the gathering of valuable insights based on the analysis of situational and contextual threats that can be tailored to the organisation-specific threat landscape. A method that could be used is Microsoft's models for the threat model called STRIDE (Swiderski and Snyder, 2004) and impact rating called DREAD (Shostack, 2008).

STRIDE is an acronym formed from the first letter of Spoofing Identity, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege that is used for describing known threats according to the type of exploits that are used. In addition, DREAD stands for Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability. By using DREAD model, the impact rating for a given threat can be determined.

Hence, the Security Analyst could explore publicly available sources of threat information. For example, we recommend that threat information approved by ENISA (ENISA, 2009) and CSA (Top Threats Working Group, 2017) be followed because there are several threats identified in these two sources. Moreover, using the STRIDE and DREAD models, actors use the following procedure to create a comprehensive threat profile:

- **Identify Threats:** the potential threats of assets that a threat agent may leverage to attack an asset. The Security Analyst needs to back up his claim with a solid foundation of Information sources.
- **Categorize Threats:** after threats and vulnerabilities have been identified, the STRIDE methodology should be used to categorize and evaluate threats according to the goals and

purposes of the attacks. By using this classification of threats, the Security Analyst can determine the category of a threat. This will provide the ability to create an impact rating for threats. STRIDE consists of the following categories:

- *Spoofing (S):* attackers masquerade as a legitimate user, system or application element.
- *Tampering (T):* attackers modify or tamper assets in transit or in-store.
- *Repudiation (R):* attackers perform actions that cannot be traced.
- *Information Disclosure (I):* breach or unauthorized access to a critical asset.
- *Denial of Service (D):* attackers disrupt or interrupt normal operations of the asset.
- *Elevation (E):* attackers obtaining access privilege to an asset without legitimate authority.

- **Target Asset:** targets systems include software, applications or configurations that are targeted and subject to exploitation by a threat.
- **Determine the Severity of Threat:** after threats are categorized according to STRIDE, the threats are rated using the DREAD model. DREAD provides a set of questions that can be applied to a scoring scheme to quantify the severity presented by threats. The questions include:
  - *Damage Potential (D):* how extensive is the damage potential?
  - *Reproducibility (R):* how easy it is for the threat to be repeated or reoccur?
  - *Exploitability (E):* how easy is it to launch the threat?
  - *Affected Users (A):* what is the estimate of users that will be affected?
  - *Discoverability (D):* how easy is it to discover the threat?

The Security Analyst can use the above questions to rate the severity of each threat. The questions can also be extended to meet an organization's need. To apply the DREAD model, a rating table is used with corresponding values of 3, 2 and 1 to represent (3) high, (2) medium and (1) low respectively. Table 4.4 shows the rating values that can be used by the Security Analyst when determining the severity of threats. The values (between 1 and 3) are counted for each threat. The result falls within the range of 5 – 15. The threats with the overall ratings of 12-15 can be treated as having 'High Severity', 8-11 as 'Medium Severity', and 5-7 as 'Low Severity'.

Table 6.7: Threat Severity

Rating	3 (High)	2 (Medium)	1 (Low)
Damage Potential (D)	The threat agent can compromise the security of an asset	Exposure to a critical asset	Minor exposure to the critical asset
Reproducibility (R)	A threat can be reproduced at any time to compromise an asset	The threat can be reproduced, but only when the opportunity is presented to compromise an asset	The threat is very unlikely to be replicated.
Exploitability (E)	A novice threat agent can easily compromise the asset within a short time.	A skilled threat agent can compromise the asset, and can easily repeat the steps	The attack requires a highly skilled threat agent, with in-depth knowledge and resources

Affected Users (A)	All users within the organisation and other customers	Some users and customers	A tiny proportion of users, and it is unlikely customers will be affected
Discoverability (D)	Vulnerabilities in the asset are very noticeable and can be easily exploited	Weaknesses in the assets are rarely discovered.	Vulnerabilities are hardly present and rarely discovered.

Table 6.8: Threat Profile

Threat ID	Threat Name	Description	Threat Category						Target Assets	Threat Severity				
			S	*T*	*R*	*I*	*D*	*E*		*D*	*R*	*E*	*A*	*D*

6.3.3.2 Step 2: Create a Risk Register

The output of threat profiling provides a list of potential security threats and the impact on assets. The threat register serves to help a Security Analyst to orchestrate the creation of a risk register and focus on the most potent threats. A risk register is an important document that provides a tentative record of potential risks in line with threat profile, assets and security goals. It will also enable the determination of how those risks are likely to occur, the severity of the risks, the steps to be taken for controlling or managing the risks, etc. (Höne and Eloff, 2002). Essentially, the Security Analyst defines an approach that makes it possible to identify, accurately estimate risks and make an informed decision about risk control actions. This will help in ensuring that minor risks are not prioritized while more severe risks are overlooked.

To ensure consistency and relevance of risks and their impact, we recommend that the Security Analyst use the OWASP risk methodology (Open Web Application Security Project, 2014) for creating the risk register. OWASP methodology is recommended for use because it estimates risks from business process and technical perspectives, highly adaptable and applicable to most organizations of all size. Six simple phases that include the factors that make up the likelihood and impact of each risk is included. The Security Analyst can then be able to use 5 phases of OWASP model to determine the severity of each risk. The phases for creating the risk register are provided as:

Phase 1: Identify Risks

The first phase deals with identifying security risks. The security analyst gathers information about the potential risks that may arise as a result of the exploitation of threats. A workshop can be organized with participants from across the organization to discuss the risks and arrive at a consensus conclusion about the general perception of risks and their impact on the organization. Also, risk details from multiple industry bodies can be considered. For example, the Open Web Application Security Project (OWASP) maintains a regularly-updated list of most pressing cloud security risks and has recently released a Cloud Top 10 Security Risks (OWASP Cloud - 10 Project, 2014). Gartner Group Inc. (Brodkin, 2008), a global research and advisory firm that provides insights, advice and tools for leaders in information technology provided a list of specific security risks that cloud users should consider before selecting a CSP. Besides, the European Network and Information Security Agency (ENISA, 2009) in a report provided a list of cloud security risks comprising 35 risks that fall under one of such categories as technical, policy and organizational, legal and non-cloud specific risks. All these sources can be used

Phase 2: Estimating Risk Likelihood

After potential risks have been identified, the next phase is to estimate the likelihood of the risk occurring. Likelihood estimation provides an approximation of how likely it is for risk to occur. OWASP has produced several factors that can be used to determine risk likelihood. However, we

recommend that the Security Analyst considers threat/vulnerability factors that focus on estimating the probability of the threats previously identified. A threat/vulnerability likelihood table is created to help the Security Analyst arrive at a sensible reasonable in determining the likelihood of risks.

Table 6.9: Risk Likelihood

Threat Factor		**0 to < 3 (Low)**	**3 to < 6 (Medium)**	**6 to 9 (High)**
Factor	**Description**			
Ease of discovery	How easy is it for the risk to be discovered?	Practically impossible	Difficult	Substantially easy
Ease of exploit	How easy is it for the risk to be exploited	Theoretical	Difficult	Substantially easy
Awareness	How well familiar are threat agents with the risk?	Unknown	Obvious	Public knowledge
Intrusion detection	How likely is the risk to be detected?	Active detection mechanisms	Logged & reviewed	Not reviewed

Phase 3: Estimating Impact for Security Goals & Business Process

In terms of estimating the impact of risks, there are two classes of impacts that can be used – technical and business impact. On the one hand, technical impacts are inclined toward the security goals of an asset that include confidentiality, integrity, availability, accountability and conformity. The aim is to provide a rough estimate of the magnitude of the impact on security goals if a risk occurs. The impact rating for technical factors is provided in Table 6.10:

Table 6.10: Security Goals Impact Table

Security Goals	**0 to < 3 (Low)**	**3 to < 6 (Medium)**	**6 to 9 (High)**
Loss of Confidentiality	Minor disclosure of critical assets	Critical assets are significantly affected	Highly critical assets are extensively affected
Loss of Integrity	Minor compromise of critical assets	Critical assets significantly compromised	All highly critical asset extensively compromised
Loss of Availability	Minor interruption of critical assets	Critical assets significantly interrupted	All critical assets extensively lost
Loss of Accountability	Threats are fully traceable	Threats are possibly traceable	Threats are completely untreatable
Loss of Conformance	A minor breach of compliance requirements	A significant breach of compliance requirements	All compliance requirements significant breached.

On the other hand, business impact estimates the severity of risks to the business process of the organisation. The Business Analyst needs to be engaged to share insights into what is vital to the organisation in running its business affairs. Further, business impact reference can be utilised to establish the processes that are important to the organisation.

Table 6.11 Risk Impact to Business Process

Business Impact		0 to < 3 (Low)	3 to < 6 (Medium)	6 to 9 (High)
Risk	**Question to ask**			
Financial damage	The extent of financial damage as a result of risk	Minor effect	Significant effect	Bankruptcy
Reputation damage	Would the risk result in reputation damage to the organization?	Minor damage	Significant damage	Loss of goodwill and brand damage
Non-compliance	How much exposure does non-compliance introduce?	Minor violation	Clear violation	High profile violation
Privacy violation	What is the consequence of disclosing personal information?	Minor consequence	Significant consequence	Highly consequential effect to privacy laws.

Phase 4: Determine Criteria for Severity of Risk

This phase involves using criteria for defining the likelihood estimate and impact estimate to calculate the overall severity for the risks. OWASP methodology uses a distributed scale of 0 to 9 for both impact and likelihood rating. The risk impact and likelihood levels are decomposed as in table 6.12 to help the Security Analyst in getting the net risk ratings.

Table 6.12 OWASP Risk Likelihood and Impact Criteria

Likelihood and Impact Levels	
0 to < 3	**LOW**
3 to < 6	**MEDIUM**
6 to 9	**HIGH**

Phase 5: Define Control Measures

There is a need to define a prioritised list of controls that can be used to address the risks. Risk controls are generic fundamental technical or procedural mechanisms that are used to manage security risks. The Security Analyst considers various industry standards that provide recommendations on basic security controls. For example, the Critical Security Controls (Centre for Internet Security, 2018) publishes a set of 20 controls and best practice guidelines that are not only limited or specific to cloud computing and which organizations should adopt to control known computer security risks.

Thus, to define control measures, we recommend that the Security Analyst selects risk control measures from the predefined list provided by a renowned industry guideline named CSC CIS (Centre for Internet Security, 2018). CSC CIS provides 20 controls categorized into 3 prioritized and defence-in-depth set of best practices that are implementable and usable to mitigate attacks against systems and networks. Further, ENISA (ENISA, 2016) provides 27 baseline security controls that are more CSP-oriented and focuses on control measures that protect cloud computing systems against operational risks. It provides a high-level security objective for CSPs with different levels of implementation of security measures. The controls provided by ENISA's are particularly used to supplement CSC CIS controls and provide expansive controls that are more specific to the cloud. Therefore, to choose security control measures,

matching is performed where each control in CSC CIS is matched to controls in ENISA to make parallel matching and identify semantic equivalence between them.

The main aim of the matching process shown in the figure is to compare security control measures from CSC CIS to ENISA, identify and filter controls that have similarities, i.e. controls that completely supplement each other in terms of scope. The elements that are used for the comparison include the name of control measure, type, and the keywords. In such cases where control measures are found to be the same, the Security Analyst should adopt CSC CIS controls. However, if there is no similarity, control measures from both CSC CIS and ENISA should be adopted. This approach ensures contents are compared more thoroughly and risk control actions consistently easily identified.

Table 6.13: Risk Register

Risk Name	**Risk ID**	**Risk Likelihood**				**Impact to Security goals**					**Impact to Business**				**Control Measures**
		EoD	EoE	Aw	I_D	Conf.	Int.	Ava.	Acc.	Con	Fin.	RD	NC	PV	

Where: *EoD = ease of discovery; EoE east of exploit; Aw = awareness; I_D = intrusion detection. Conf = confidentiality; Int. = integrity; Aav = availability; Acc = accountability; conf = conformance. Fin = financial; RD = reputation damage; RD = noncompliance; PV = privacy violation*

6.3.4 Activity 4: Requirements Specification

The output of the previous activity provided a risk register, detailing an overview of various security risks facing an organisation and control measures for addressing risks. As stated earlier, control measures are well-vetted security actions which organisations can take to ensure the protection of assets from various kinds of harms that may be mounted by several types of attackers. This activity encompasses more details, mainly by considering security controls from different perspectives and techniques. In particular, it focuses on establishing broad security controls that do not only focus on addressing security risks but also for ensuring security transparency. In identifying requirements, the vital spectrum of cloud operations is considered such as security transparency requirements, baseline security requirements, compliance requirements etc. By considering all aspects of security requirements, the audit will be more comprehensive and elaborate to cover the verification of many aspects of an organisation's requirements. Therefore, the primary objective of this activity is to specify essential security requirements that mandate the presence of control measures around assets are reiterated and identified to ensure sufficient coverage in the management of cloud services.

6.3.4.1 Step 1: Specify Transparency and other Requirements

In this step, the actual requirements that serve as essential constraints that must be satisfied by the CSP are specified. The security analyst is involved to specify asset requirements in a documented matrix formally. The requirements are primarily specified according to four different aspects: security transparency requirements, baseline requirements, business requirements, and operational requirements. The requirements are derived from well-known industry standards to support a set of accurate and verifiable and implementable controls that are driven from standard practice. Essentially, industry-acclaimed CSA CCM Version 3.0.1 (Cloud Security Alliance Control Matrix, 2016). CSA CCM provides sixteen essential security principles that guide CSPs on achieving cloud security and also provides organisations with the structure to achieve asset security in the cloud. Therefore, we recommend that the Security Analyst creates a categorised list of requirements based on CCM to specify the requirements that are relevant to the organisation.

Table 6**.14** Requirements Specification

Requirements	Control Domain	Control Type	Control ID	Specification
Transparency				
Basic				
Business				
Operational				

6.3.5 Activity 5: Assess CSP

After essential security requirements have been identified, the Security Analyst needs to assess the reliability worthiness of a CSP in terms of their capability to provide satisfy security requirements. The purpose of this activity is to evaluate commercially available CSPs and determine the most suitable one that can fulfil security, business, and requirements. The activity is necessary because the

propensity to provide transparent services can vary from one CSP to another, and while transparency assurances are reputedly given, there are no guarantees these assurances can be nurtured and sustained by the CSP. Although very essential, the activity is more pertinent for organisations that are yet to migrate their backend assets to the cloud and somewhat optional for organisations that have already moved to the cloud. Thus, the outcome of this activity is to support decision making in respect of choosing an appropriate CSP. This activity, therefore, contains two steps, including the collection and assessment of the evidence.

6.3.5.1 Step 1: Collect CSP Information before Migration

This step provides organizations with the chance to, before migration, select a suitable CSP or if already migrated, determine the security transparency worthiness of an existing one. Most of the commercially available CSPs usually specify or reveal the featured attributes of transparency within their services and stated as promises that will be fulfilled. Occasionally, organisations tend to put trust on CSPs based on reputation or experience of other users. The rationale behind this step is to gather adequate background information relating to CSPs' transparency that significantly helps organisations to have a greater assurance on how security requirements are fulfilled and how risks are controlled. To achieve this, assurance information about as many CSPs have to be collected for comparison purposes to identify the most suitable candidate that can deliver security transparency. There are a variety of ways that can be used for collecting information. A method for collecting information proposed in this research involves a detailed search of prospective CSPs' web portal for collecting information about their approach to security transparency. In addition, existing assessment offered by professional industry body, namely: CSA CloudTrust Protocol (CloudSecurityAlliance, 2010) can be leveraged. Table 6.15 provides an insight into the type of information that can be collected for every requirement and the possible sources.

Table 6.15 Type and Sources of Information

Requirement	Type of information	Source of Information
Transparency	Availability	The web portal, CSP attestation, industry accreditation & certifications.
	Clarity	
	Current	
	Relevance	
	Notification	
	Verifiable	
	Free/low cost	
	Independent third-party audits	
	Incident Reporting	
Business	Business Continuity Plans	The web portal, security whitepapers, CloudTrust Protocol, CSP attestation, third-party audit report, industry accreditation & certification
	Policies and regulatory regulations	
	Risk management	
	Security governance	
Basic	Network / Infrastructure Services	The web portal, security whitepapers, CloudTrust Protocol, CSP attestation, third-party audit report, industry accreditation & certification
	Encryption & key management	
	Sensitive Data Protection	
	Unauthorized Software Installations	
	Identity & access management	
	Application & Interface Security	

	Controlled Access Points	
Operational	Vulnerability / Patch Management	The web portal, security whitepapers, CloudTrust Protocol, CSP attestation, third-party audit report, industry accreditation & certification
	Infrastructure & virtualisation security	
	Handling information leakage	
	Data Security Integrity measures	
	Datacentre Security User Access	

6.3.5.2 Step 2: Perform Assessment

Statements regarding the elements of security transparency made by CSPs need to be assessed and verified to support decision making for selecting the trustworthy CSP. In this step, the Security Analyst estimates CSPs based on predefined measurement questions proposed in this thesis. The questions are formulated according to the principles of security transparency as presented in Chapter Four (such as availability, clarity, current, relevance, etc.). Moreover, a measurement metric is created to aid the determination of a score that can be assigned to one or multiple candidates CSPs. The measurement metric uses a 'Yes' or 'No' for assigning score value to the distinctive questions. If the answer to a question is 'Yes', then a value of 1 is assigned, meaning that the CSP has achieved an aspect of security transparency relating to that question. A 'No' answer attracts a value of 0 meaning that the CSP does not meet the respective principle of security transparency in that regard. A measurement criterion that reflects the deployment practices of security transparency (i.e. opaque and explicit transparency) is applied for determining the type of security transparency proffered by each CSP.

In the measurement criteria, a value of 1 to 7 is applied to determine the CSP transparency type. A CSP with a score of ≤ 3 is considered to have 'Opaque Transparency', whereas a CSP with a score of more than $\geq$ to provides explicit transparency. The assessment is applied in guiding the judgement of the Security Analyst to determine: (i effectively), before cloud migration, select the most suitable CSP; (ii) or if already migrated, determine the transparency worthiness of an existing CSP. Table 6.16 shows security transparency principles. The assessment is helped by criteria as shown in table 6.17. The result of CSP assessment is reported to top management to consider and deliberate on the most suitable CSP that should be adopted. It is essential to mention that the migration activities are not covered in this research.

Table 6.16 Assessment Questions of CSPs

Security Transparency Principle	Relevant Question	CSPs Assessed		
		CSP1	CSP2	CSP..
Availability	Is information published regarding the security controls and policies of the CSP?			
Clarity	Is the information published in a way that can be easily interpreted by customers?			
Current	Does the CSP publish up-to-date information regarding changes to policies, practices and security events/incidents?			
Relevance	Does the CSP publish relevant information that can support customers to elicit requirements and perform risk assessments?			
Notification	Does the CSP provide timely notification services/tools for reporting security events, incidents or operations concerning customer assets?			
Verifiable	Does the CSP provide verifiable system-generated activity logs?			

Free/Low cost	Does the CSP provide information at low/free cost?			
	Total Score			
	Transparency Type			

Table 6.17: Criteria for Transparency

Score Value	Transparency Type	Criteria
≤ 3	Opaque	Information is not well clarified. It involves CSP disclosing information that either partially represents its actual operational values or provides equivocal statements. Also, inconsistent or unreliable information in terms of how controls are actualised in the cloud environment
≥ 4	Explicit	Information is disclosed to represents a realistic implementation of CSP security control, precisely outlines the processes and procedures of how operations are securely managed. Comprehensive elucidation on the CSP's approach to ensuring the protection assets is provided

Let:
Transparency = TR; Availability = AV; Clarity = CL; Current – CU; Relevance = RE; Notification = NT; Verifiable = VR; and Free = FR

Hence,

$$TR = AV + CL + CU + RE + NT + VR + FR$$

If:

TR is ≥ 4, then CSP transparency is Explicit.

Else:

TR is ≤ 3, then CSP transparency is Opaque.

6.3.6 Activity 6: Security Audit

This is another vital activity that is performed after cloud migration has taken place. It introduces an ongoing audit process that is aimed at assisting organizations in examining whether the CSP continuously and effectively implements plans, procedures and controls that meet organizational security requirements for protecting assets once cloud migration has been successfully achieved. The audit process presented in this activity uses ISO/IEC 19011:2018 and ISAE 3402 Audit Standards. It is initiated by the Security Auditor to collect evidence, independently evaluate the CSP's fulfilment of security transparency and controls based on the evidence collected, and prepare a substantive audit report to the organization's actors. The activity consists of steps as (i) define the security requirement to be audited; (ii) collect evidence in respect of the security requirement; (iii) analyze evidence; (iv) and issue a report. Audit evidence collection implies the reliable collection of relevant evidence through inspection, inquiry or observation. The analysis deals with examining collected evidence to establish whether security requirements are being implemented. Reporting mainly involves documenting findings and building judgments based on evidence collected. The main output of the activity is to measure the conformance or nonconformance and determine the areas where a CSP must implement controls. The steps involved are described below:

6.3.6.1 Step 1: Define the Requirements to be audited

This step specifies the focus and depth of the audit in terms of the specific requirements and CSP security controls that are subject to verification. Hence, the security requirements specified in the preceding activity are considered and become the focal point of consideration. In addition, defining the security requirements to be audited allows the collection of evidence that is most relevant for the control areas which are under scrutiny. For example, an organization that had specified incident management and reporting as a requirement will need to collect, analyze and examine evidence that focuses on the incident management and reporting controls implemented by the CSP, and therefore, form the scope of the audit.

6.3.6.2 Step 2: Collect Audit Evidence for the Requirements to be audited

This step involves gathering documentary evidence or historical records about the CSP's platform to assert proof of conformance to the organisation's security requirements and other operational integrity. According to the guidelines for audit evidence collection in ISAE 500 Standard (ISAE500), an auditor must obtain sufficient appropriate evidence to afford a reasonable basis for forming a judgement. In this context, the evidence is reliable, relevant and adequate electronic records, computations, and client or third-party representations about the implementation of processes, procedures and mechanisms needed to secure the cloud platform and fulfil requirements. Evidence also provides all the information that can be used by an auditor to arrive at a conclusion. Audit evidence is assessed to allow security auditor to produce audit findings and present findings. The importance of collecting evidence artefacts is that it supports assertions, statements and claims about how individual requirements and CSP controls are met. Thus, in the course of this step, we have identified essential evidence that the Security Auditor needs to collect, the sources from where evidence is to be collected and method for obtaining the evidence.

6.3.6.2.1 Technique for Evidence Collection

To collect evidence, it is recommended that the security auditor uses a checklist that is primarily designed to support the collection of evidence. The checklist comprises a series of questions that are relevant to the security requirements. The intent for using the checklist is to have a uniform means for obtaining adequate information and assurance from the CSP regarding security practices. The questions in the checklist are formed by considering industry-accepted initiative namely: Consensus Assessments Initiative Questionnaire (CAIQ V3.0.1) (Cloud Security Alliance, 2017b) and Critical Security Controls (CIS) (Centre for Internet Security, 2018).

CAIQ provides a series of 'Yes' or 'No' questions that are aligned to control areas of CCM and which an auditor may ask of a CSP in assessing the capabilities and competencies of the CSP. It promotes the use of best practices for providing security assurance in cloud computing. Also, another distinguishing feature of CAIQ is that it is mapped to several industry-accepted security standards,

regulations and control frameworks that are mostly of interest to both CSPs and cloud users. On the other hand, CIS provides a set of actions and best practices for controlling most common attacks against systems and networks. Controls in CIS are derived from most common attack patterns highlighted in the leading threat reports and vetted across a broad community of industry practitioners. An important reason for considering CIS is the fact that it provides defence-in-depth for risks that are non-specific to the cloud.

The questions in the checklist are categorised according to security domains and subdomains. Each subdomain contains several questions that must be answered by the CSP. The CSP responds to the questions with 'Yes', 'No' or 'Not applicable'. Where 'Yes' response is obtained for a specific question in the checklist, the CSP must produce evidence to support their assertion concerning that question. A 'No' and 'Not applicable' answers do not require supporting evidence from the CSP.

6.3.6.2.1 Evidence Type

Under different circumstances, different types of evidence can be collected and each varies according to the requirement that is subject to audit. Some evidence pertains security and event logs, while other forms of evidence entail proof of CSP certifications/accreditation from standards/frameworks. In terms of security and event logs, the Security Auditor focuses on logs about applications, user activities, and security incidents etc. which contain information related to events that have occurred within the cloud environment. Such logs are generated by various cloud components, including penetration testing, vulnerability scans, intrusion detection and prevention systems, servers, applications and network equipment. Therefore, the types of logs collected are directly relevant and correlate with the security requirements that are subject to audit. In other words, the kind of event log collected is dependent on the context of the particular question in the checklist and security requirements. For example, for an organisation whose requirement include virtualisation security, logs from virtual machine security monitoring software provide useful data that could be of use in detecting malicious activity and verifying CSP's conformance to such requirement.

Table 6.18: Types of Evidence to be collected

Evidence Category	Specific Evidence
	Login attempts to disabled service/suspended accounts
Authentication and Authorisation Monitoring Report.	Login failures and successes by users and systems
	Multiple login failures
	Privileged account Access (Success/Failures)
	User authentication failures
Critical Failures and Errors Monitoring Report	Critical failures by virtual machines, operating systems, and applications
	A virtual machine, system and application crashes, shutdowns, restarts
	Backup failures
	Capacity exhaustion for memory, disk, CPU and other system resources
	Additions of accounts to administrator/privileged groups
	Additions/changes/deletion to users/groups
	Additions/changes/deletions to network services

Data and Systems Change Monitoring Report	Applications install and updates by systems, applications and users
	Changes in file access permissions
	Changes to sensitive files
	Changes to system and configuration files
	Password changes and resets by users and administrators
Malware Activity Monitoring Report	Anti-virus protection failures
	Connections to known malware IP addresses
	Events from anti-virus tools
	Malware detection trends with outcomes
Network Activity Monitoring Report	Antivirus and antimalware log file
	Data loss prevention event log
	Firewall log files
	Honeypot logs
	Intrusion detection and prevention system log files
	VPN activity log files
Resource Access and Activity Reports	Application log files
	Event log files
	Service log files
	System logs files
	Virtual machine log files
Certifications/Accreditations from Frameworks and Standards	Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR)
	Control Objectives for Information and Related Technology (COBIT)
	European Network and Information Security Agency (ENISA) Information Assurance Framework (IAF)
	European Union Data Protection Directive (EUDPD)
	Federal Financial Institutions Examination Council (FFIEC)
	Federal Information Security Management Act (FISMA)
	Federal Risk and Authorisation Management Program (FEdRAMP)
	Health Information Portability and Accountability Act (HIPAA)/ Health Information Technology for Economic and Clinical Health (HITECH)
	Health Information Trust Alliance (HITRUST)
	International Organisation for Standardisation (ISO27001:2005)
	International Traffic in Arms Regulations (ITAR)
	NIST Cybersecurity Framework
	North American Electric Reliability Corporation (NERC)
	Payment Card Industry Data Security Standard (PCI DSS)
	Sarbanes-Oxley (SOX)
	Statement on Standards for Attestation Engagements 16 (SSAE 16)

6.3.6.2.2 Source of Audit Evidence

The sources a Security Auditor can explore for collecting evidence depends on the context of security requirement. Ideally, log files are a vital source of evidence and provide measurable benefits in monitoring and analysis of events of any system. Logs can be seen as a rich source of evidence because they provide detailed information about activities being performed and help to determine whether everything is working as desired. However, the monitoring and management of logs, especially in a distributed environment, require considerable resources for analysis and correlation. For example, the sources of evidence for specific security requirements such as human resources security cannot be obtained through logs, while security requirements such as threat and vulnerability management require automated tools and techniques such as penetration testing. Hence, a combination of sources is used depending on the security requirement under scrutiny including CSP assertions; security whitepaper; website information; user experience, CSP audit report, and reports generated by security and monitoring tools.

6.3.6.3 Step 3: Perform Security Audit

Once evidence is collected, the next task is to perform the audit work following ISA 200 and ISA 402 (ISA, 2016) standards. Specifically, the audit involves analyzing evidence in an attempt to evaluate and establish the conformance or non-conformance of CSP controls, i.e. determine whether security procedures and practices in the CSP's environment sufficiently safeguard assets and comply with security requirements of the organization. To achieve this, the checklist created in the previous step serves as the reference point for reviewing CSP practices and the extent to which the CSP conforms to the organization's requirements.

6.3.6.3.1 Apply Audit Criteria

Audit criteria is a set of procedures, policies, specifications, or requirements used as a reference against which evidence are compared. The audit criteria can be qualitative or quantitative, general or specific, focusing on what should be according to laws regulations or objectives, sound principles, scientific knowledge or best practices (ISA, 2016). In performing an audit, the Security Auditor uses justifiable audit criteria or select from standard procedures and policies. Reliable sources of audit criteria could be regulations, legislation and standards issued by recognized authorities. For ensuring that evidence is presented in conformance with generally accepted principles, the Statement on Auditing Standards 70 (American Institute of Certified Public Accountants. Auditing Standards Board, 1997) provides essential attributes that are paramount for evaluating the quality of audit evidence and to support the reasonable basis for auditors opinion. Thus, these attributes (as shown in Table 6.19) are adopted and reformed to the context of cloud audit to serve as the audit criteria for assessing evidence. The attributes are considered on the supposition that credence must be established in respect of whether CSP security practices and procedures are done in accordance to specified requirements.

Table 6.19: Attributes for Quality Audit Evidence (Audit Criteria)

Parameter	Description
Sufficiency	Quality evidence is sufficient quantity has been presented to support assertions made on specific security controls.
Completeness	The CSP has presented evidence of all security processes and procedures relating to security controls
Understandability	Implementation of security controls, processes and procedures are appropriately presented and described, and disclosures are clearly expressed.
Accuracy	Data presented and disclosures made relating to security controls, procedures and processes accurately reflect instances of the cloud operating environment.
Reliability	The source of evidence is reliable by nature and is dependent on the individual specific security control area under which it is obtained.

6.3.6.3.2 Step 2: Determine Conformance Level

This step involves assessing CSP evidence and performing appropriate analysis to form an opinion that is presented in the audit report. The primary aim is to establish the conformance level associated

with the CSP's practices based on the evidence produced. In other terms, once a CSP has supplied evidence, an auditor uses professional judgement to measure the sufficiency, reliability and completeness of evidence, and its understandability and accuracy. Essentially, to establish a CSP's conformance level, a thorough assessment of all evidence presented by the CSP is performed. The evaluation mainly determines the CSP's conformance in respect of requirements. A simple equation and an assessment scorecard are created, where the Security Auditor, based on expert analysis and interpretation, determines the level of conformance that is associated with a CSP, i.e. the ability to satisfy security requirements. In other words, after evidence have been analyzed and assigned a score about the attributes of quality evidence, a computation is performed to determine the CSP's level of conformance to the security requirements.

i. ***Conformance Level to each Question*:** using the scorecard in Table 6.20, the Security Auditor assesses evidence presented by the CSP and assigns a value of either '1' or '0' according to how each evidence satisfies the attribute of quality evidence (SCUAR). For example, assuming a CSP had responded with a 'Yes' answer to a question and also presented supporting evidence, an auditor assesses the quality of the evidence in terms of its sufficiency, reliability, completeness, understandability and accuracy. If the auditor perceives evidence to validate the CSP's claim, then he scores the evidence with '1', otherwise '0'.

$$\boldsymbol{Conf.Level} = \frac{\text{Sufficiency+Ccompleteness+Understandability+Accuracy+Reliability}}{\text{5 (Attributes of Quality Evidence)}} * 100$$

Table 6.20: Evidence Scorecard:

Attributes of Quality Evidence	Possible Values	Score Value for Evidences
Sufficiency	1 or 0	Score = 1 if 'Evidence is Sufficient', else Score = 0
Reliability	1 or 0	Score = 1 if 'Evidence is Reliable', else Score = 0
Completeness	1 or 0	Score = 1 if ''Evidence is Complete, else Score = 0
Understandability	1 or 0	Score = 1 if ''Evidence is Understandable, else Score = 0
Accuracy	1 or 0	Score = 1 if 'Evidence is Accurate, else Score = 0

Table 6.21 General Scorecard for CSP Conformity Level

Conformance Type	Weight	Conformance Level
Very High conformance	100	5
High conformance	80	4
Medium conformance	60	3
Low conformance	40	2
Very low conformance	20	1
Nonconformity	0	0

Table 6.**22** Security Audit/Analysis

Requirement	Target Verification (Control Domain)	Base Measure (Control Type)	Specification	Question	CSP/User Response		Means of Verification	Audit Criteria					Conformance Level
					Yes	No		S	C	U	A	R	

* Sufficiency; completeness; understandability; accuracy; transparency

Table 6.22 provides evidence analysis and audit report. The target verification implies the set of control domains being assessed. For an auditor to perform the required assessments, a base measure is used, that is the type of control being audited. For instance, evidence produced in respect of the application and interface security within (target of verification) to manifest what controls exist in the area of data integrity (i.e. base measure). Therefore, application and interface security become the target of verification, whereas data integrity controls under application and interface security become the target of verification. Furthermore, the means of verification implies the type of evidence that was examined, i.e. supporting evidence produced by the CSP such as log report generated by automated security monitoring tools. The audit criteria highlight the audit criteria (attributes of quality evidence) upon which evidence is compared. Each evidence obtained is compared to the criteria for determining a certain weight or score that will be associated with the evidence. Assessment score assigns a score value to the evidence that has been analysed. Total score cumulates the overall score attained by individual evidence for the base measure in respect of all five audit criteria. Global score cumulates the overall score achieved target verification (control domain) in respect of base measures. The Conformity level determines the level of conformity a CSP has achieved. The outcome is a summary of findings to support the auditor in generating an audit report.

6.3.6.4 Step 4: Report Audit Findings

An audit report is defined as a written opinion or decision of an auditor based on overall findings. It is the primary means for communicating results of the audit to relevant actors, and in some instances, also shared with to the CSP. The contents of the report focus on the organisation's requirements that have been assessed and the degree to which the CSP is meeting such requirements. In other words, after auditing the requirements of an organisation (such as transparency or fundamental requirements), the auditor needs to create a report regarding the finding that has been discovered during the audit. For instance, do the results show weak controls or flawed fulfilment of requirements? Are the requirements and controls determined to be effective and efficiently fulfilled? Once these considerations are established, remedial actions that must be implemented by the CSP are drawn by the auditor. The remedial actions take different perspective including, measures that are designed to pre-empt irregularities before they occur; measures that identify defects, threats or errors on a timely basis after they have occurred; measures that correct defects or risks and prevent further reoccurrence; or auditor statement indicating sufficient and satisfactory controls not needing further actions. In general, the report prepared by the Security Auditor presents findings and weaknesses discovered and recommendations for remedying deficiencies found. The audit report fulfils many objectives, including formally presenting findings; serve as a statement of assurance; and the identification of areas requiring remedial actions on operations, controls or policies and procedures that must be implemented.

To ensure consistent reporting according to an established process, the audit report is developed based on the provisions and in compliance with information security audit standards and audit protocols. In

particular, the guidance for audit reporting in ISA 700 (International Standard on Auditing, 2016) are followed. The standard maintains that the audit report should be understandable and presented in a logical order, can communicate the scope, objectives, results and recommendations of the audit, and also to assist the organisation to take corrective actions. As a general rule, the audit report contains the auditee (organisation) and intended actors, the scope and extent of the audit work, findings, conclusions and recommendations. Therefore, based on the outcome of the previous step, the Security Auditor creates a report detailing audit findings and opinion. The reports contain certain information, and the structure within which the contents are presented is driven by the need to make reports readable and understandable. Hence, the audit report is drafted by considering important aspects, including:

- **Audit Requirements:** provides a statement of the audit area covered, i.e. what aspect of CSP control as contained in the checklist is audited. In other words, it reflects on the security requirements. For example, if the audit covered encryption and key management: key generation control domain only, then encryption and key management: storage and access should be excluded from the report.
- **Audit Conclusion/Judgement:** this provides an overall judgement regarding audit findings in respect of each requirement and the CSP's security controls. In other words, once evidence has been examined, compared against the audit criteria and assigned a weighted score, the auditor provides a judgement concerning their findings. For example, the auditor might have discovered nonconformance in an area of fundamental security. In this instance, the auditor must state that CSP practices were found to be inadequate or ineffective for the requirement in question. There are three types of judgements that an auditor, having obtained sufficient audit findings, an issue to establish judgment, which includes defective, acceptable and effective controls.
    - **Defective Practice:** this type of judgement is presented in cases where the audit findings substantially indicate material disparities between audit criteria and CSP asserted evidence. From another perspective, defective controls are audit findings where adequate controls are not in effect, or there is a reasonable doubt that security requirements are being met.
    - **Acceptable Practice:** this judgement is issued when audit findings indicate similarity between audit criteria and CSP assert evidence, but there are disparities or weaknesses in certain areas. In another perspective, acceptable controls imply audit findings where security controls are in place to provide acceptable assurance; however, controls need to be tightened or improved in some areas.
    - **Effective Practice:** judgement is presented when audit findings indicate a substantial correlation between audit criteria and evidence. From another perspective, effective

controls manifest the presence of all security controls, procedures and practices are in place following relevant security requirements and applicable criteria.

- **Remedial Action:** action plans are constructive recommendations issued by the auditor when the audit findings substantiate significant improvements in operations and performance of the CSP. The main intention is to recommend changes to areas of requirements where non-conformance has been observing or where significant weaknesses in controls are found. Remedial Action is mainly issued using corrective, detective or preventive actions. The responsibility for implementing remedial action could rest on the CSP or an organization. From both the CSP and organizational perspective, remedial actions are recommended to make sure the necessary measures implemented to address the lack of fulfilling requirements or insufficient controls.
    - **Preventive**: include security control measures, policies, and procedures that are to deter or prevent security incidents, risks, errors, or omission of requirements from occurring.
    - **Detective:** technical and non-technical security controls, policies, procedures that detect errors or incidents and provide visibility into malicious breaches and attacks.
    - **Corrective:** technical implementations and procedures that mitigate damage, correct errors or incidents once they have occurred.

6.4 Chapter Summary

This chapter presented an integrated and unified process for the security transparency framework, which involves multiple activities, steps, and decisions to achieve successful implementation from the organizational point of view. The process comprises four fundamental activities, with various steps connected to each activity. It leverages several industry standards to provide the basis of defining and achieving specific goals, mitigating threats, and establishing controls per established best practices. The combination of various standards and best practices ensures higher efficiency, compliance and reduces the potentials of errors and failures, which also reduces the tendency of repetition.

Table 6.23: Report Audit Findings

Requirement	Target Verification (Control Domain)	Base Measure (Control Type)	Question	Audit Judgement			Remedial Actions		
				Defective	Acceptable	Effective	Preventive	Detective	Corrective

CHAPTER SEVEN

Security Transparency Audit Tool (STAT)

7.1 Introduction

The previous Chapter presented a process for CSTF, which comprises various fundamental activities and steps. The final activity of the process involves a security audit that focuses on assessing CSPs and establishing whether they effectively implement the necessary procedures and controls that meet organizational requirements continuously. In this Chapter, the design of STAT is presented in detail, which is designed to support auditors in the performance of a security audit. In plain terms, STAT is designed to serve as a platform by which an organisation can probe the activities of a CSP by seeking information about specific requirements, receive evidence about how the CSP meets the requirements, and establishing assurances about the degree to which CSP fulfils requirements. The primary objective of STAT is to facilitate the collection and analysis of evidence, including the establishment of subjective audit judgement and determination of the required course of actions that needs to be taken, thereby promoting security transparency in the cloud.

Therefore, this chapter is intended to convey the significant architectural considerations used in building STAT. It presents details of the features, specification and implementation outline of the tool. The chapter uses non-technical to mildly-technical terms to make it more comprehensive and understandable by providing an overview, general description, design process, and features of the tool. Also, high-level details for the overall design of STAT in terms of functional architecture, as well as the relationship between various modules and functions of the tool are provided. Also, a description of its essential functionalities and features is provided through an explanation of the many dashboards of the tool.

7.2 Overview of STAT

STAT is designed to be a supporting audit tool for CSTF that an organisation, in particular, auditors can use to perform a security audit. It is designed to enable auditors to leverage a security audit checklist that is formed on the principles of renowned industry-standard to probe CSP services, collect and analyse evidence, and produce findings regarding CSP's conformance to requirements. Another vital aspect of STAT is that it aims to focus on many aspects of specific organizational requirements. This process is enabled through a query-response approach that is initiated and controlled by an auditor on behalf of an organisation, where the CSP responds to a request by supplying relevant evidence.

7.3 STAT's Intelligent Scoring and Assessment System Architecture

Various engines have been designed and integrated for use by STAT to provide intelligent capabilities for assessing and computing CSPs' conformance level to an organisation's requirement based on the evidence presented by the CSP. The intelligent module of STAT

comprises of various engines such as registration and requirement manager. This section provides a brief description of STAT's internal components.

7.3.1 Registration Engine

The registration engine (RE) allows CSPs to register and provide service specifications related to an organisation's requirement, responding to the assessment checklist that is developed using the CAIQ, and supplying relevant evidence. The RE captures all details and inputs from the CSP and forwards the service specifications, CPS response and evidence to the Transparency Data (TD) and the Conformance Level Assessment Engine (CLAE) for further processing respectively.

7.3.2 Requirement Manager

The Requirement Manager (RM) provides a front-end to stakeholders for supporting the specification of relevant requirements that are subject to assessment before determining the conformance level of a CSP. Based on the requirement specified by stakeholders, the RM determines the conformance score of CPS by using the Transparency Engine (TE) and the Transparency Computation Engine (TCE). By default, stakeholders can receive the overall conformance level associated with a CSP based on the completion of the checklist. Otherwise, stakeholders can customize preferences of conformance level of CSP according to requirement.

7.3.3 Transparency Engine

The Transparency Engine (TE) is responsible for converting all transparency-related data into propositional logic (AND, OR) to model and formalize the variables that determine whether a CSP conforms to a particular requirement or set of requirements. The TE is built based on subjective probability using CertainTrust Model (Ries, 2007) that allows making decisions in the context of uncertainty using two representation parameters namely independent parameters (consisting of an estimated probability of trustworthy behaviour) Bayesian approach that uses beta probability density functions. CertainTrust models the reliability of an entity based on one's belief that a certain proposition is true.

7.3.4 Conformance Level Assessment Engine

The Conformance Level Assessment Engine (CLAE) consists of the checklist that is designed to enable CSPs to provide details and evidence on their capabilities to address an organisation's requirement. The questions in the checklist are designed to be answered in 'yes' or 'no' format, categorised as control domain (CD) and all the questions regarding CDs are stored in the Transparency Data (TD). The CLAE is designed based on the assumption that a CSP provides only one set of valid response, while the auditors are responsible for checking the validity and authenticity of the answered checklist using the variables in the audit criteria. Also, CLAE

considers evidence presented by the CSP as proof of requirement attainment and audit criteria are used as the basis for conformance scoring factors in the engine, which comprises the following equations and accompanying rules:

The overall conformance score C_s(in %) of a CSP is computed by:

$$C_S = \left[\frac{\sum_{i=1}^{k} C_D}{k}\right] \qquad (1)$$

Where:

C_r = conformance score with regard to a C_D as computed by (2),
k = number of requirements

The conformance score C_s (in %) concerning a C_D is computed by:

$$C_S = \frac{\left(\sum_{i=1}^{m} ActualC_{Di}\right)}{\sum_{i=1}^{m} TotalC_{qi}} * 100 \qquad (2)$$

Where:

$ActualC_q$ = actual conformance score concerning question q of Control Domain C_D as computed by (3)
$TotalC_q$ = possible total conformance score concerning a question q of Control Domain C_D as computed by (3),
m = number of questions of Control Domain C_D.

The conformance score Cq (in %) for each question q is computed by:

$$C_q = \frac{\left(\sum_{i=1}^{p} ActualC_{mi}\right)}{\sum_{i=1}^{p} TotalC_{mi}} * 100 \qquad (3)$$

Where:

Actual C_m = actual conformance score concerning criteria m of question q as computed by (4)
$TotalC_m$ = possible total conformance score concerning criteria m of question q as computed by (4)
P = number of criteria of question q

The conformance score C_s (in %) about a criteria m is computed by

$$C_S = \frac{\left(\sum_{i=1}^{r}(C_{ei}*W_{sf}) + \sum_{i=1}^{r}(C_{ei}*W_{re}) + \sum_{i=1}^{r}(C_{ei}*W_{cp}) + \sum_{i=1}^{r}(C_{ei}*W_{ud}) + \sum_{i=1}^{r}(C_{ei}*W_{ac}) +\right)}{(\max(W_{cl}))*r} * 100$$

(4)

Where:

S_e = existence score of evidence e that is associated with criteria m (that is if evidence exists score = 1, else score = 0)
W_{sf} = Sufficiency of evidence as in Table 6.20
W_{re} = Reliability of evidence as in Table 6.20
W_{cp} = Completeness of evidence as in Table 6.20
W_{ud} = Understandability of evidence as in Table 6.20
W_{ac} = Accuracy of evidence as in Table 6.20
Max_{cl} = Conformance Level as in Table 6.20
R = number of evidence associated with criteria m

In addition, intelligent assessment and scoring rules have been designed for use by STAT to provide the basis for computing an appropriate conformance level of CSP to organisation's requirements. The rules consider the inputs of security auditors for the requirements, control domains and control types

Rule 1:

For all control domains CD_1, CD_2… CD_n. if the conformance level of control domain in requirement *A* are the same as those of requirements B, then the overall conformance level of requirement *A* should be equal to that of *B.* Assume we have control domains in requirement A with a set of CD = {*CD1* CD_1, CD_2… CD_n.}, where CD represents the *x*th control domain, the compliance level for requirement *A* on the control domain CD_x is represented as C_A^{CDx} whereas the overall compliance level of requirement A is $C_A^{Overall}$. This rule is formally defined as If ∀ $CD_i \in CD$, $C_A^{CDi} = C_B^{CDi} \Rightarrow C_A^{Overall} = C_B^{Overall}$

Rule 2:

If for control domain $CD_1 \ldots CD_k$, requirements *A* and requirements *B* have the same compliance levels, and for other requirements $CD_{k+1}, \ldots CD_n$, the compliance level for requirement A are higher than those of requirement B, then the overall score of *A* should be higher than that of *B*. This rule is formally defined as:

$If \forall CDi \in \{ CD_1, \ldots CDk \}$, $C_A^{CDi} = C_B^{CDi}$ and

$\forall CD_x \in \{CD_{1+1}, \ldots CD_n \}$, $C_A^{CDx} > C_B^{CDx} \Rightarrow C_A^{Overall} > C_B^{Overall}$

Rule 3:

For control domain, CD_i, for which the compliance level of a requirement *A* is higher than that of requirement *B,* and also there exists control domain CD_x, for which the compliance level of requirement A is lower than that of B.

Rule 4:

If there exist *m* requirements (R_1, R_2, … R_m) where $m > 2$, the overall compliance score between requirements will follow the 2 previous rules outlined above, which is formally defined as:

Given multiple requirements such as (R_1, R_2… R_m),

for p = 1: m – 1

for q = p + 1 : m

compute C_p^{Overal} and C_q^{Overal} *following rule* $1 \sim 2$

based on the evidence provided by the CSP.

7.3.4 Audit Decision with Subjective Logic

Auditors' judgement and opinion regarding the conformance level of CSP which are formed on the assessments generated by CLAE using subjective logic. Subjective logic is a trust algebra based on Bayesian theory and Boolean logic, which is used to explicitly model uncertainties (Jøsang, 2016). It represents a specific belief calculus that uses a metric called opinion to express beliefs, where an opinion *x* is denoted by $\omega_x^A = (b, d, u, a)$ expresses the relying party A's belief in the truth of statement *x.* Binomial logic is applied to binomial opinions that are represented by quadruples of real numbers $\omega_x = (b_x, d_x, u_x, a_x)$ within an interval of [0…1] subject to constant $b_x + d_x + u_x + a_x = 1$, which refer to *belief, disbelief, uncertainty* and atomicity of x. Further, subjective logic operators are applied in aggregating the opinion of different auditors over a period of assessments. Barycentric coordinates are then used to aggregate and visualize opinions. As mentioned earlier, binomial opinions are calculated based on the assessment results from CLAE that considers CSPs response to the checklist and overall auditors' opinion.

The Auditors' opinion is determined by applying fuzzy concepts to a Barycentric coordinate to have a classification for every opinion using 3 rating classes for the opinion, which include: very effective, effective, very acceptable, acceptable, defective, and very defective as shown in Table 7.1.

Table 7.1: Classification of Opinion

Region	Belief	Disbelief	Uncertain
Very effective	$b_x \geq 0.5$	$d_x \geq 0.5$	$u_x \leq 0.5$
Effective	$0.25 \leq b_x \geq 0.5$	$d_x \geq 0.25$	$u_x \leq 0.5$
Very acceptable	$b_x \geq 0.5$	$d_x \geq 0.5$	$u_x \leq 0.5$
Acceptable	$b_x \geq 0.25$	$0.25 \leq d_x \leq 0.25$	$u_x \leq 0.5$
Defective	$0.25 \leq b_x \leq 0.25$	$0.25 \leq d_x \leq 0.25$	$u_x \leq 0.5$
Very defective	$d_x \leq 0.25$	$d_x \leq 0.25$	$u_x \leq 0.25$

7.3.4.1 Quantifying Audit Judgement

By assessing evidence provided by CSPs through CLAE, auditors are allowed to establish judgement based on CSP responses to the checklist. Auditor's judgement $\omega_x^A = (b, d, u, a)$ is quantified using addition aggregation factor $\lambda \in [0, 1]$. The value of λ is the factor that controls the rapidity of time by either increasing or decreasing it, and therefore, the aggregation does not affect judgement if $\lambda = 0$ and is entirely neglected after a single time period, while also having the largest effect of $\lambda = 1$. Thus,

- $r_{y,t}$ denotes the conformance level generated for CSP for requirement *y*
- $R_{y,t}^x$ Implies the conformance level based on auditor *x* judgement and CSPs response over time *t* for requirement *y.*

- $R^{x}_{y,(t+1)}$ Implies the general conformance level for CSP based on auditor *x* judgement after time period t + 1 for requirement *y*.

Furthermore, auditors are permitted to perform an assessment of any number of time and a method to perform this option is created. The method considers the judgement established by an auditor *x* towards requirement *y* based on the previous judgement k_t as well as the current judgement k_{t+1}. The rationale behind this consideration is based on the fact that performing another assessment strengthens auditors' judgement in terms of a CSPs conformance level and produces well-founded judgement. Therefore, assuming the previous judgement of an auditor is $k_t = 0$, the new judgement $R_{y,(t+1)}$ after a period of time t + 1 can be expressed as:

- For the first auditor assessment: $R_{y,(t+1)} = \lambda + r_{y,t}$ where $0 \leq \lambda \leq 1$, $\lambda = (k_{t+1} - k_t)\lambda$
- For any auditor assessment but not the first one: $R_{y,(t+1)} = \lambda + R_{y,t}$ where $0 \leq \lambda \leq 1$, $\lambda = R^{x}_{y,(t+1)} - k_t\,\lambda$

Therefore, the overall conformance level determined by all auditors $x \in X$, where *X* implies the set of all auditors judgement that performed the assessments – can be generated from the overall average judgement of as:

$$R^{x}_{y,(t+1)} = \frac{\sum x \in \mathrm{X}\, R^{x}_{y,(t+1)}}{[X]}$$

The value of *k* can be determined as:

- For very effective judgement and certain class ($k = 1$)
- For effective judgement and certain class ($k = \frac{1}{2}$)
- For very acceptable judgement and certain class ($k = 1$)
- For acceptable judgement and certain class ($k = \frac{1}{2}$)
- For defective and certain class ($k = -1$)
- For very defective and certain class ($k = -\frac{1}{2}$)

7.3 General Description of STAT

STAT is a web-based front end that is written in open-source programs using PHP (Lerdorf et al., 2006), HTML5 (Hickson and Hyatt, 2011), and MySQL database (Glass et al., 2004). The client-side can be accessed using a standard browser, and it will be able to run on any web server that supports PHP and has a MySQL database. It consists of administrative, server and user modules. For the administrative and user interfaces, JavaServer Pages (JSP) (Hall, 2001) is used for displaying pages, and MySQL for retrieving, inserting, deleting and updating data in the database. This setup enables multiple users to log in and interacts with the tool simultaneously.

Also, STAT is developed using two user levels – administrative and user levels. The first type of user is the administrator who can set up and change system settings and user privileges. The second user is the basic users that consist of auditors and CSPs, who can only perform operations assigned by the administrator. The tool comprises several different components, which can be

directly accessed based on the access rights of users. Each web page is associated with certain aspects of security audit activity and provides important functionalities to manage evidence collection, analysis and generation of a report. Importantly, the web pages communicate with each other through a common database that is built using MySQL.

7.4 Design Process

In designing STAT, vital considerations are made regarding the most important aspects of the audit activity and forming the tool's features around these considerations. Several architectural designs were considered including a distributed system that utilises client-server web service technology, and distributed systems using PHP. For each architectural design, the pros and cons were considered, including feasibility and capability to cope with the features of the tool. For example, the architectural pattern in web services technologies is lightweight. Distributed systems, create more cohesion and increase the degree of interdependence between modules. PHP is a server-side scripting language that is independent, multi-platform, and would allow the tool to be more coupled, which implies that the client will be more dependent upon the server-side. Thus, after thorough consideration and proof of concepts, it is decided for the tool to be implemented as a client-server web system that will be designed using PHP.

7.5 Architecture of STAT

In this section, the architecture of the tool is explained. STAT is a simple three-tier, web-based system that uses a client-server architecture. A three-tier architecture is an architecture pattern for developing web applications which work around three important layers, comprising a presentation layer, application layer and data layer (Conallen, 2002). Three-tier architecture is used to improve the modularity of the tool, and particularly allow for easy extension of features. Using client-server architecture, users can use any web browser to connect to the many services supported by the tool such as initiating audit assessments. On the server-side, the web server receives requests from the client, handles the request and generates an appropriate response to the client. The three-tier architecture role of three-tier architecture is explained as:

7.5.1 Presentation Layer

The presentation layer provides visualisation and dashboards that enable an organisation, security auditors and CSPs to interact with the tool, and enables the visualisation of audit information of various kinds such as assessment results, conformance level etc. It specifically provides the necessary user interface to enable auditors and CSPs' access and use the tool using a standard browser. This layer is built using HTML, PHP and JavaScript, and it consists of web-browsers for HTTP clients that efficiently interact with the application and data layers using standardised protocols.

7.5.2 Application Layer

The application layer is built using PHP, and it essentially plays the role of linking together all the three layers by technically processing the various inputs and selections received at the presentation layer, and interacting with the vast database in the third layer. It houses the audit assessment module/platform, which specifically applies an algorithm to auditor's assessment of CSPs to determine appropriate conformance level. It is also responsible for determining access rights of auditors, generating and managing access codes sent to CSPs. Also, the layer houses the web server, scripting language and the scripting language engine of the tool. The Web server enables the processing of HTTP requests for initiating the audit process, obtaining CSP responses and evidence. The application layer provides the technical deal with dynamic content and streamlines faster access of the database to extract results.

7.5.3 Database Layer

The database provides a centralised place where data captured in the tool are stored, manipulated, and accessed. The layer comprises database management systems (DBMS) and the database, which is built using MySQL. The rationale for the database layer is to centralise all data storage and retrieval duties concerning security audit, user profiles, authentication, audit history, etc. In other words, it contains the methods for accessing the underlying database data. Fundamentally, the database layer is responsible for storing numerous types of data the tool will take as an input, generate as output and other external services that the tool may use. The database is accessible to the system administrators and auditors. The high-level architecture for the tool is shown in Fig. 7.1.

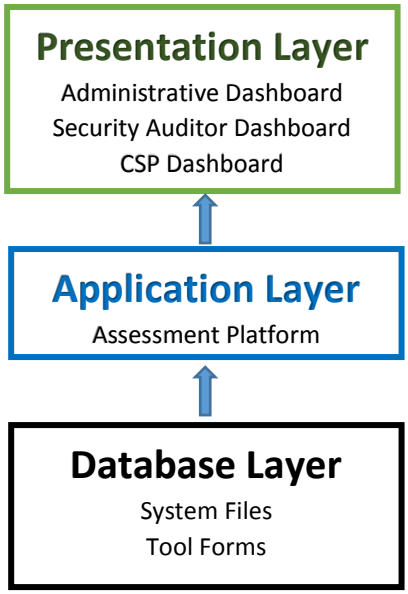

Figure 7.1 Architecture of STAT

7.6 Features of STAT

A detailed overview of STAT features is provided in this section. The primary purpose is to provide a general understanding of how the tool is decomposed and how the individual components work together to provide the desired functionalities. Generally, the tool focuses on the evidence-based way of probing, assessing and reporting of findings relating to CSP conformity to requirements. The main features provided by the tool include three main dashboards consisting of essential functions that can be performed. Each functionality contains important components of a security audit. The three main features include administrative client; security auditor; CSP dashboards as shown in Fig. 8.2

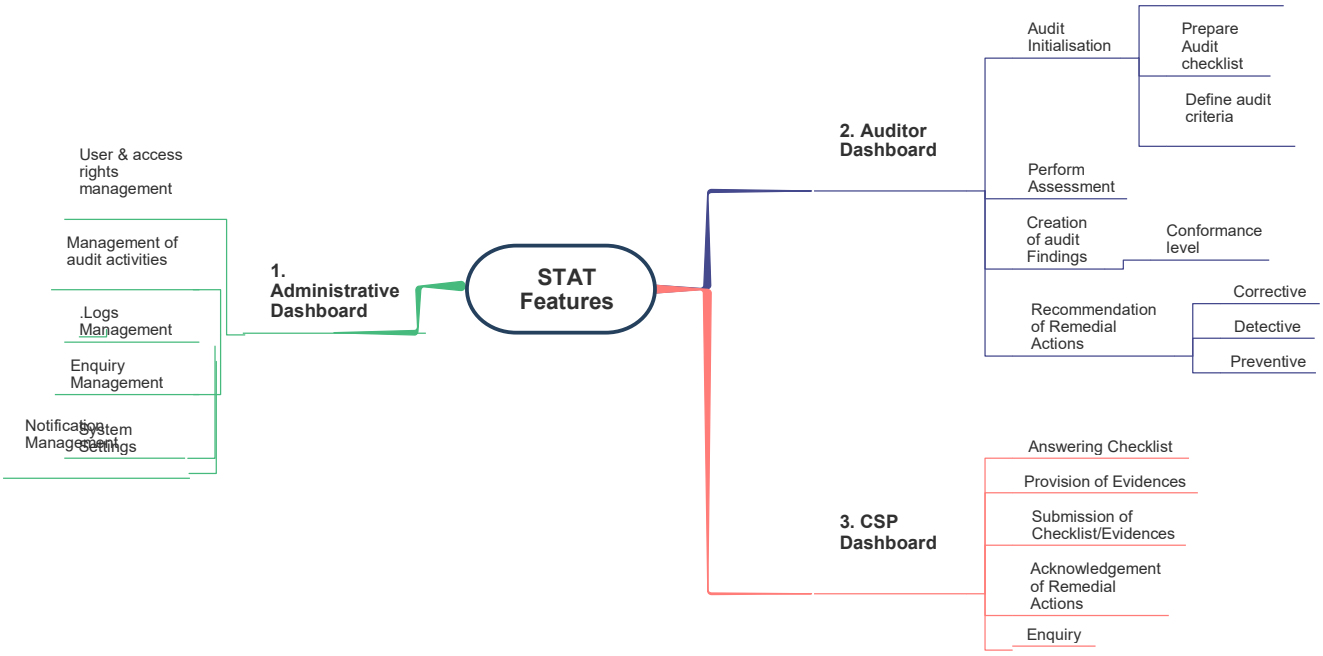

Figure 8.2: Features and components of STAT

7.6.1 Administrative Dashboard

The purpose of this feature is to provide administrative and user management functions in terms of authentication and providing auditors and CSPs access to the STAT platform. The authentication module is designed using PHP with MySQL database, which serves as an integral part of security procedures. The primary user of this dashboard is the STAT administrator who creates user accounts for all authorised auditors and the CSP whose services are subject to assessment. The administrative dashboard also enables the auditor to manage logs and user activities in terms of reviewing auditor activities and CSP profile. Also, it allows the management of enquiry from the CSP who may have some questions, complaint, suggestion, and submission of requirements or checklist regarding the assessment. The system administrator can add, remove or edit the list of auditors that can use the tool, in addition to password recovery capabilities.

Among other functions the administrative dashboard allows the auditor to maintain the overall system security, functionalities and definition of user access rights; create of user account; management of auditors assessment invitation to CSPs; control of audit platform; verification of CSP details and assessment invitation before being sent out by security auditors; notification services on completion of assessment, CSP response management, and acknowledgement of remedial plans by CSP.

7.6.2 Security Auditor Dashboard

Security Auditor Dashboard provides an auditor with the functionalities to perform a systematic assessment of CSPs conformity to requirements. It consists of many features that enable the auditor to establish requirements that will be audited, prepare security audit checklist, initiate the assessment process, gather and evaluate evidence from a CSP, establish and communicate the findings, and recommend remedial actions upon the completion of the assessment. Another important functionality provided by this feature is to enable an auditor to initiate the security audit by establishing contact with an inviting the CSP to commence the audit. This is achieved using an assessment invitation form that is embedded in the tool and managed by STAT administrator.

The form consists of important details including the CSP's name, the email address provided and the requirements that are being audited. This is followed by a request being sent to the CSP through a secure hyperlink and access credentials. The access credentials enable the CSP to log into STAT platform and access the checklist. In other words, the assessment invitation is automatically sent out to the CSP in a secure hyperlink that directly connects to the universal resource locator (URL) of the security audit checklist which comprises numerous questions prepared by the auditor

Essentially, the auditor dashboard provides an interactive page for access to the default checklist that is composed of a predefined set of questions derived from industry standards, which is stored in the STAT platform. The focus of the checklist is the requirements that will be audited, with each requirement consisting of standard properties such as control domain, control type, question, CSP/user response and the type of evidence supplied by the CSP. Moreover, an auditor can modify the default checklist by adding, deleting or changing the questions. This is particularly important in situations where the auditor has identified the need to improve the dynamicity of the checklist or adaptive to the business context of the organisation. In case of modification, changes to the checklist are saved, encoded and sent to the MySQL server for storing.

7.6.3 CSP Dashboard

This is the feature that enables CSPs to participate in the assessment routine. The goal is to provide the capabilities for a CSP to access STAT platform and take part in the audit process by responding to questions in the checklist. In other words, it allows the CSP to answer the checklist with a view of providing evidence and enabling the cloud auditor to assess responses and evidence

provided. Once the CSP acknowledged the audit invitation sent by STAT administrator, access permission is granted using credentials issued by the administrator. The checklist then appears as a form, covering the requirements that have been earlier defined by the auditor. The CSP then answers the set of questions relevant to each requirement using a dual-type checkbox that allows them to toggle between two choices – 'Yes' or 'No'. Also, the evidence must be supplied by the CSP for every question that is answered with a "Yes" response. This is done by uploading and submitting documentary evidence that supports the CSPs' assertion. Also, the dashboard allows the CSP to enquire the assessment or any other form of question they may have for the auditor. Lastly, audit findings and remedial actions recommended by the auditor are received by the CSP through this dashboard, who in return acknowledges and report back on the measures being taken to address the recommended actions.

7.7 STAT Workflow

This section provides a summarised narration of the steps and functions involved in the application of STAT with a view of helping users have an understanding of how the tool is used. The whole process is described in Fig 8.3.

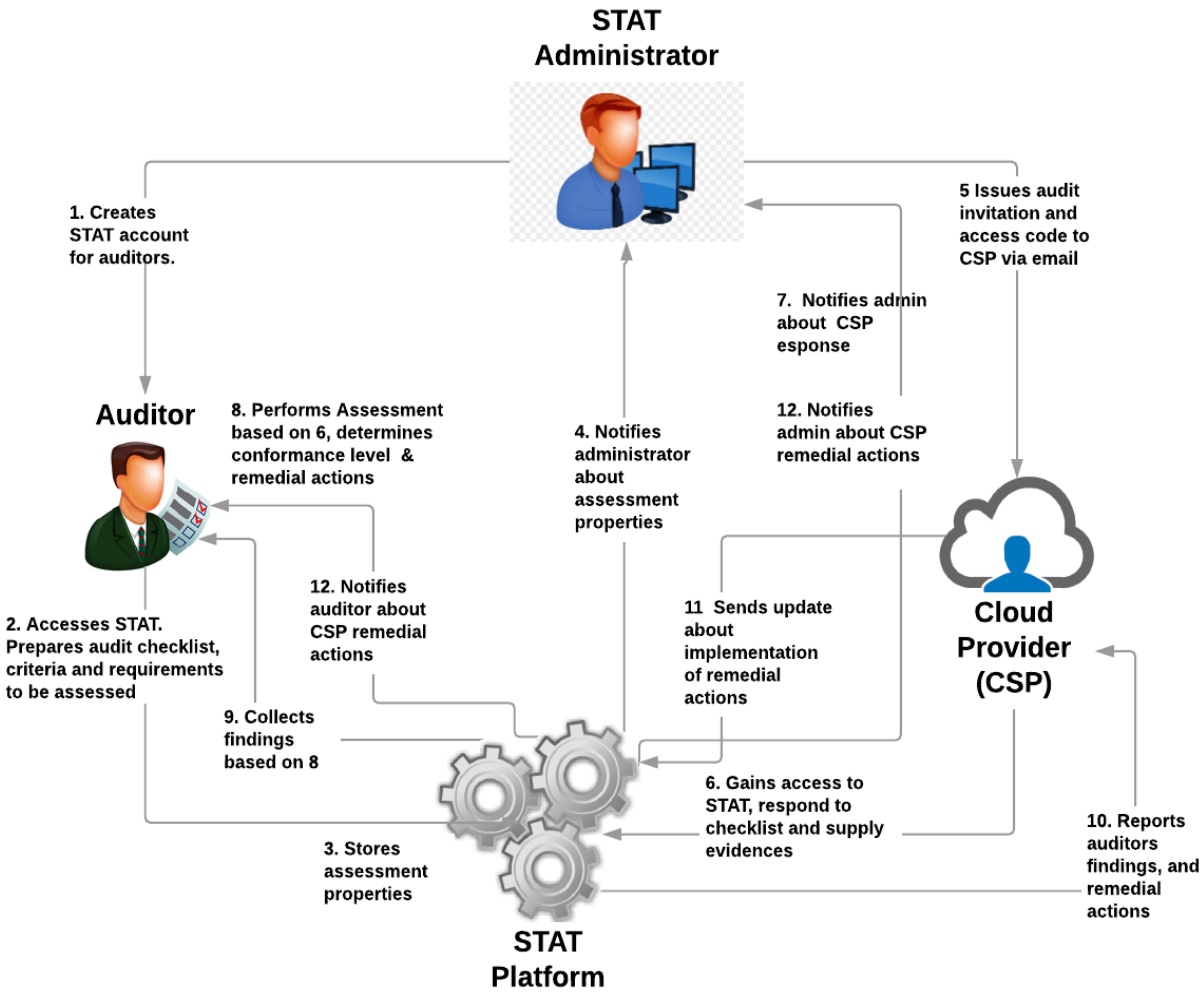

Figure 7.3: STAT Workflow

1. Once the tool is set up and configured, the STAT administrator creates a user account for an auditor that is charged with the responsibility of performing the assessment. Details such as name and email address are used for identifying the auditor;
2. The auditor is issued login credentials for access to STAT platform, and the option to manage account settings and preferences. The auditor begins the assessment preparations by creating or using an existing audit checklist and assessment criteria, as well as selecting the company requirements that will be audited;
3. The assessment properties prepared by the auditor are then stored in the STAT platform;
4. The STAT administrator receives an instant notification about the completion of the auditor's assessment properties, who then;
5. Confirms the assessment properties and sends out an assessment invitation to the CSP through an email address of the CSP, containing a secure hyperlink and access credentials;
6. When logged in, the CSP views the checklist form, provide responses, attach evidence where necessary and sends back to STAT platform;
7. The STAT administrator receives the CSPs submitted checklist and evidence and notifies the auditor;
8. Subsequently, the auditor begins the assessment by examining CSP responses, comparing evidence to audit criteria and determine a CSP's conformance level based on an assessment of the evidence. In addition, the auditor generates assessment findings and establish remedial actions that must be implemented by the CSP;
9. STAT platform collects findings and remedial actions;
10. Sends a report to the CSP detailing findings and remedial actions that must be implemented;
11. The CSP continuously sends an updated report about the implementation of remedial action; and
12. STAT feeds the administrator about CSP update, who in turn notifies the auditor.

7.7.1 Dashboard Views

A preliminary view of the major dashboards in STAT is presented in this section. The interface uses a straightforward plain layout with very little or no graphics. Information is displayed very clearly to users through HTML pages, with visualisation mechanisms that present information using graphical aids such as charts. As mentioned earlier, there are four main dashboards in STAT. First, the administrative dashboard, the auditor dashboard and the CSP dashboard. Screenshots from these dashboards are provided as below:

7.7.2 Administrative Dashboard

7.7.2.1 Admin Login:

This page enables STAT Administrator to log in with valid and authorised email address and password to carry out the task of administering Security Auditors and CSP's and other important tasks on the dashboard. This page uses a sha256 Salt Hash Security mechanism to run a session check and transmit a valid or invalid result. If session check is valid, it means that the Administrator has provided a valid login credential and is being logged in to a secure dashboard page "index.php" if session check is invalid it means that the login details provided by the Administrator are invalid thereby prompting an Error message and redirecting the Admin to a Login page "login.php" to try again with the correct login credentials.

Url: http://statportal.cbfnewsafrica.com
Email: admin@admin.com
Password: admin001

Figure 7.4: Admin Login

7.7.3.2 Admin Home Page

This is the official landing page of the Admin if successfully logged in, and it comprises of the data display sheet with summed up figures of the CSP's, the Auditors and the Audit requirements. To the left are the menu options navigable to linked pages and with various tasks.

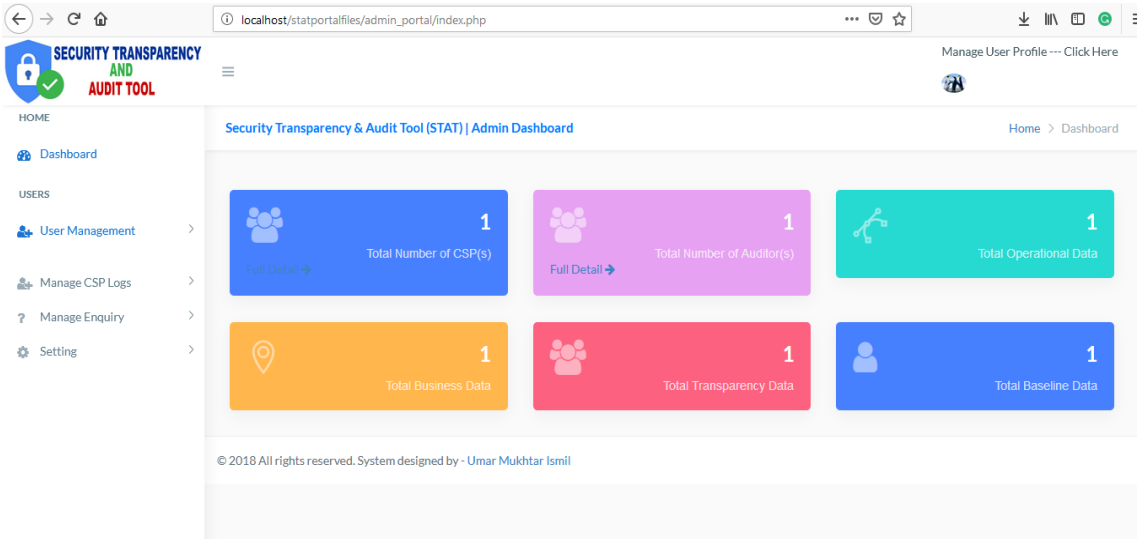

Figure 7.5: Admin Home

7.7.3.2 User Account Management

User management i.e. (Create Security Auditor and CSP Accounts) through the "View Users Account" the admin can perform account management actions such as edit, delete or add a user

View User Accounts Url: view_all_users.php

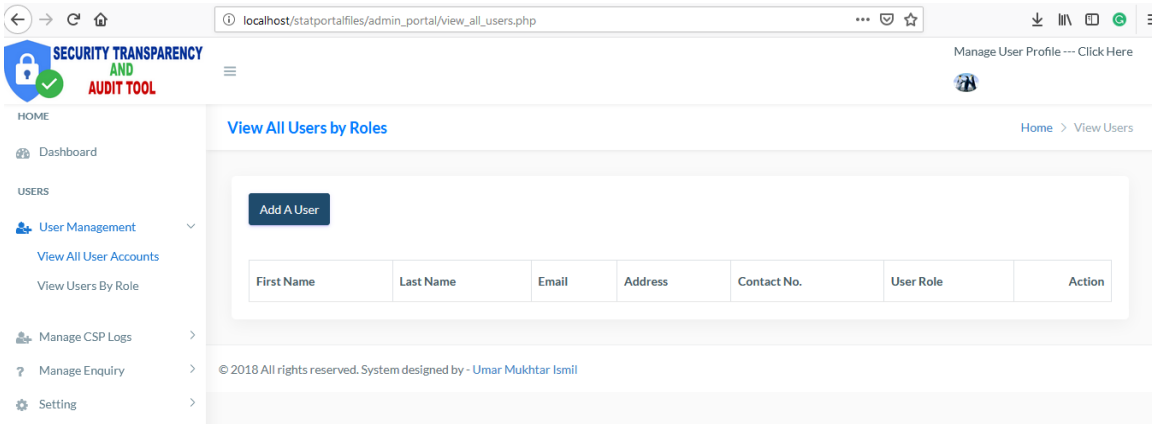

Figure 7.6: Viewing user accounts

Furthermore, the user account management enables the admin to add or create a user either as a "Security Auditor or as a CSP", after filling the form, the admin is prompted to select a user role to enable the system to create a new user based on assigned role.

Add User Account Url: add_user.php

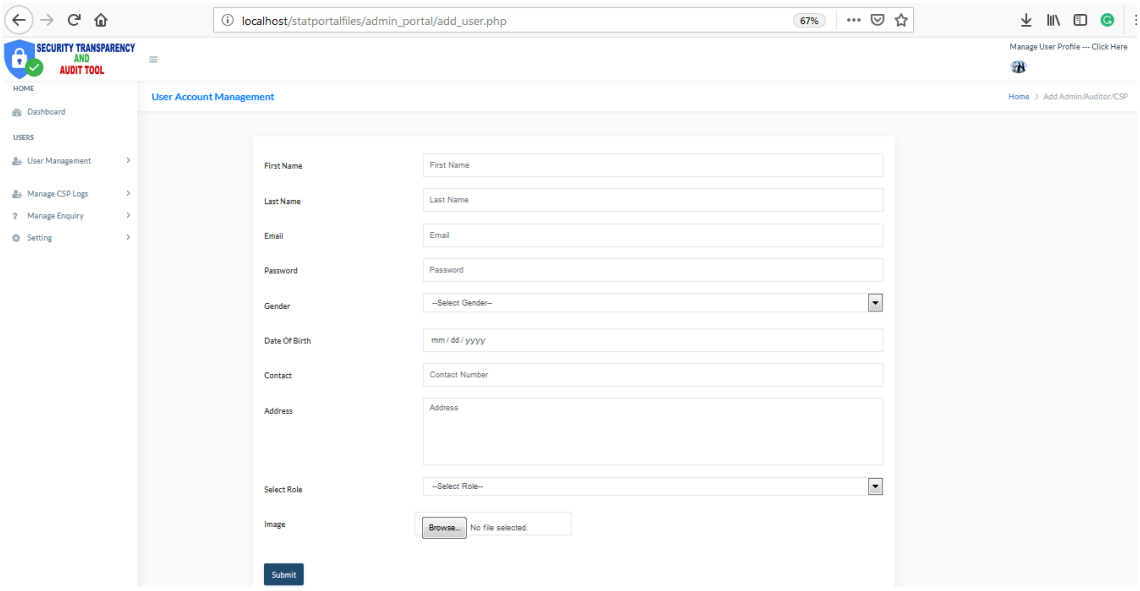

Figure. 7.7: Adding user accounts

7.7.3.3 Managing User Logs (Security Auditor/CSPs)

This section enables the Admin to keep track of the particular task or actions being carried out by either a Security Auditor or the CSP. When a user is online, the status is represented by 1 when offline the status is 0. Also, is the log of the time and date of a user's last visit and the most visited page and tasks performed

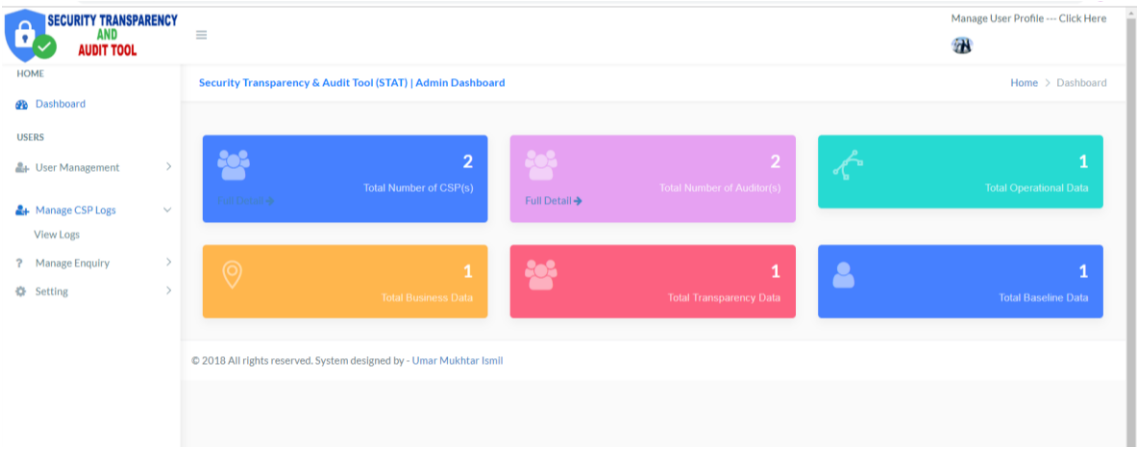

Figure 7.8 Managing User Logs

7.7.3.4 Manage Enquiry:

This page enables the administrator to view all enquiry entries generated by the CSP. An enquiry may come in the form of a complaint, suggestion, submission of requirements or checklist etc. each submission by a user is tracked by the system's database and transmitted to the administrator in descending order with enquiry subject, date and time of submission.

View Enquiry Url: view_enquiry.php

7.7.3.5 STAT Configuration Settings

This feature comprises of some of the key components of STAT that allows the administrator to perform configuration settings such as email configuration and Short Messaging Services (SMS) configuration for sending and receiving assessment alerts. The Email configuration entails the Email settings, Mail delivery Host, Mail port, Mail Username, Mail Password and Mail encryption. The Short Messaging Services involves the Sender ID, Username, Password and the Authentication Key.

7.7.4 Security Auditor Dashboard

7.4.4.1 Security Auditor Authentication

This page enables the Security Auditor to log in with valid and authorised email address and password to carry out the task of assessing the checklists, requirements, criteria's, results/findings and taking remedial actions through the assessment dashboard. This page uses a Hash MD5 Security mechanism to run a session check and transmit a valid or invalid result. It also allows an auditor to gain access into the system by creating a new account with a preferred username, email address and password, the system processes the registration and verifies the authenticity of the username and email and its availability on the database "statportal_db" and table "auditor_user".

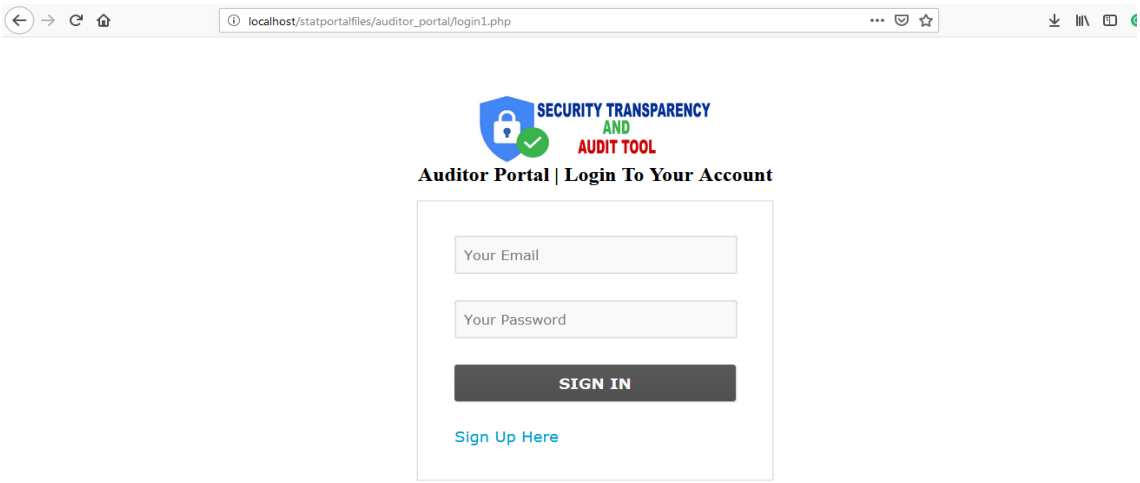

Figure 7.9: Security Auditor Authentication Form

7.7.4.2 Security Auditor Dashboard

Security Audit Dashboard provides the primary features of the assessment. It comprises of the data display sheet with summed up figures of the CSP's, the Auditors and the Audit checklist requirements. To the left are the menu options navigable to linked pages and with various tasks.

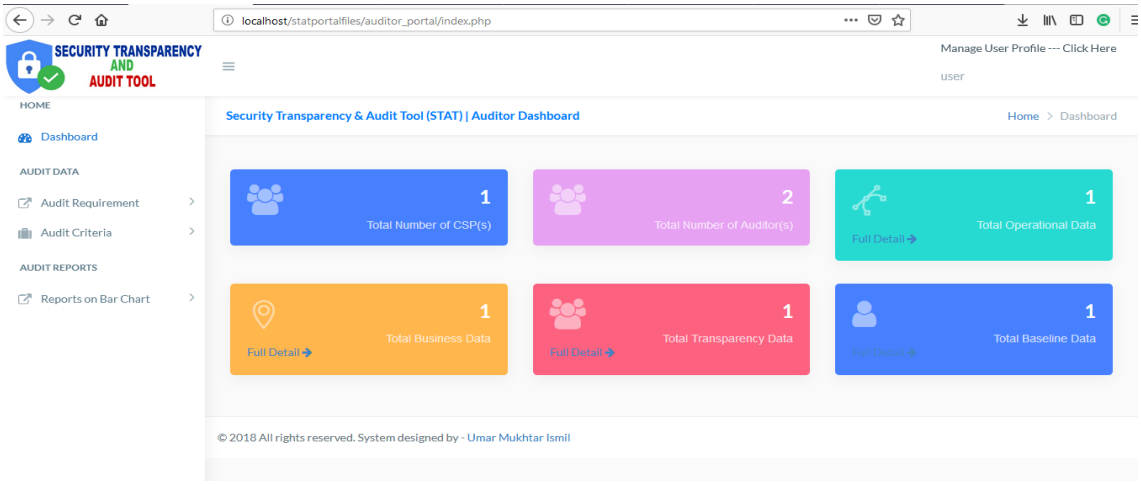

Figure 7.10: Security Auditor Dashboard

7.7.4.2 Audit Checklist

This is the primary dashboard that allows the security auditor to select the requirements that will be assessed from a list of required options such as baseline, transparency, business, and operational, and prepare the audit checklist. The requirement and its checklist data are stored and retrieved from database name "statportal_db" database tables "tbl_baseline", "tbl_transparency", "tbl_business_data", "tbl_operational_data".

The dashboard also enables the security auditor to make changes to the checklist by adding, editing, and deleting the overall or individual question within the checklist. After completion, the checklists are then stored in the STAT platform to be accessed by the CSP for a response. STAT administrator is then notified about the completion of the checklists by the security auditor.

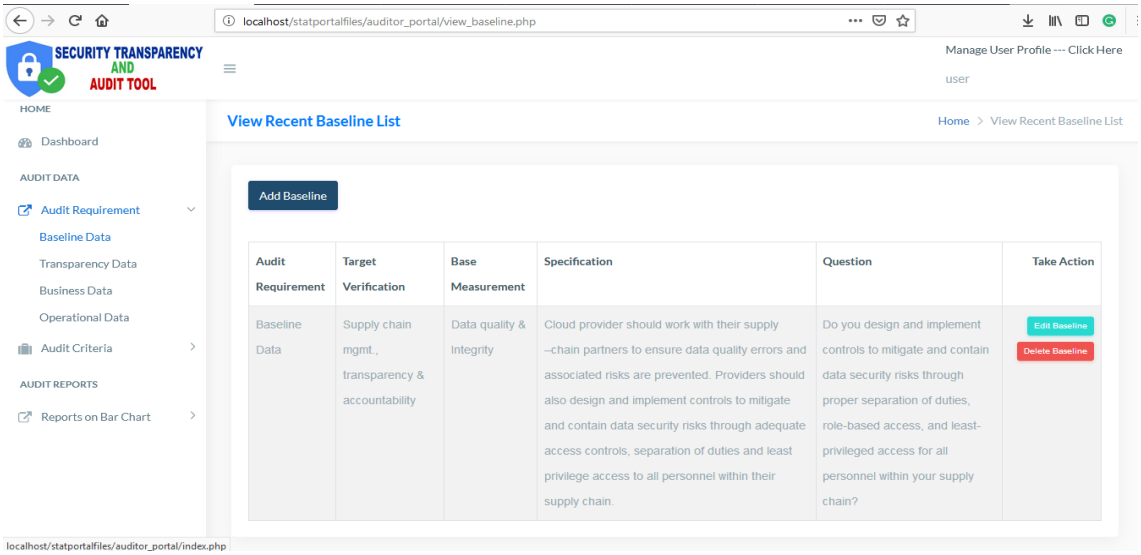

Figure 7.11: Creating a Checklist

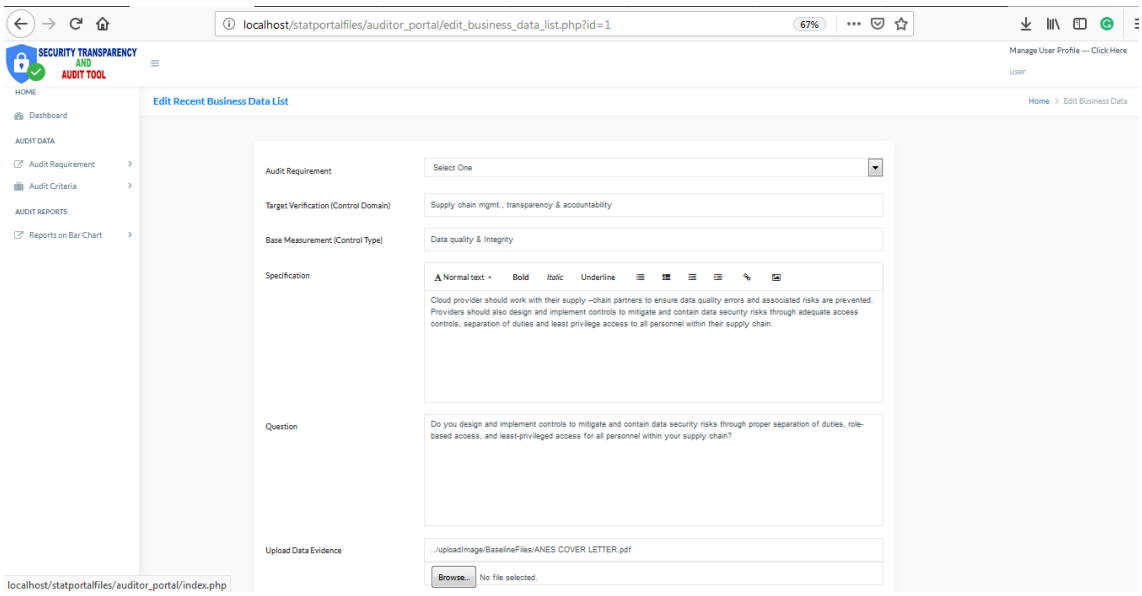

Figure 7.12: Adding Questions to Checklists

7.7.4.2 Audit Criteria

This feature allows the security auditor to define and establish the audit criteria that will be used for assessing CSP responses and evidence supplied. The system merges the CSP User database table "csp_user" with the Checklist/Criteria database tables "tbl_baseline", "tbl_transparency", "tbl_business_data", "tbl_operational_data" to check and track the answered checklist/criteria with each CSP's User ID's. It therefore tremendously reduces the workload of the security auditor by providing accurate records and a transparent auditing process; it also enables the security auditor to spend less time assessing and providing responses and remarks to its Answered Checklist criteria.

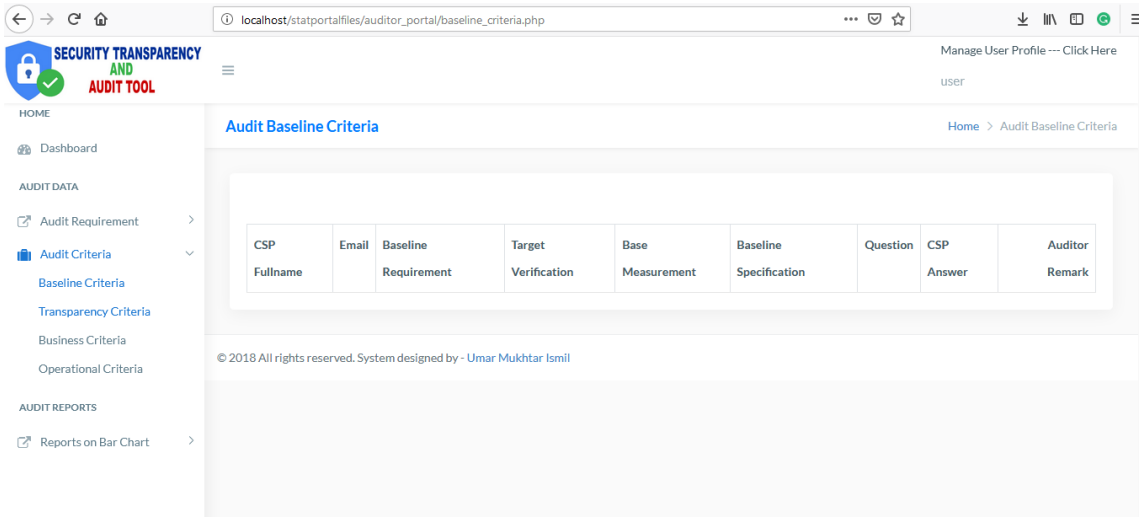

Figure 7.13: Preparing Audit Criteria

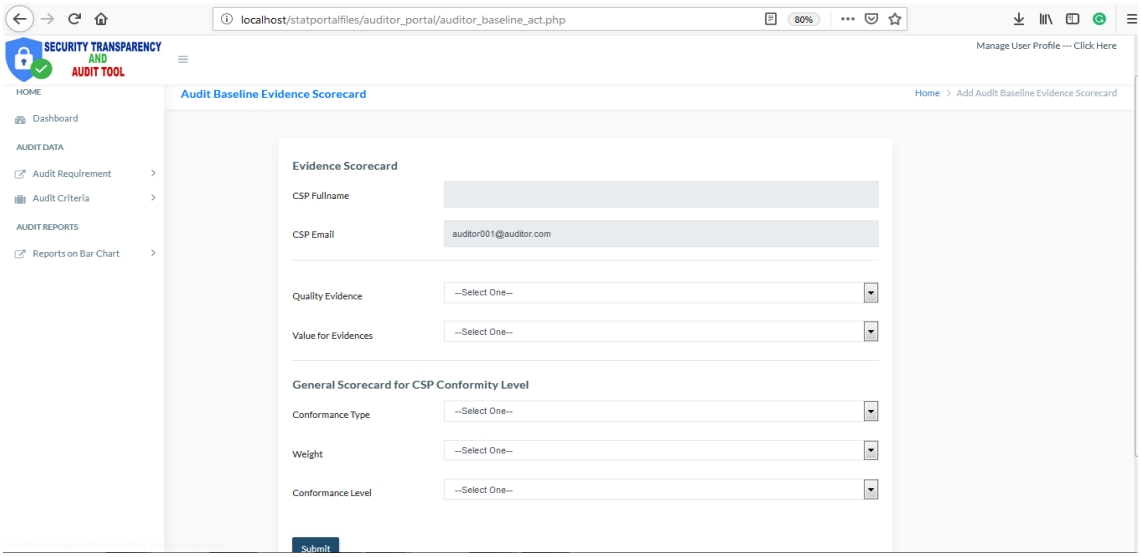

Figure 7.14: Audit Criteria

7.7.4.3 Audit Report/Findings

STAT allows an auditor to generate audit findings based on the assessments performed. Assessment findings are done compiled by the auditor detailing the conformance level achieved by the CSP. A bar chart data sheet is used for displaying the results for a more accurate and simplified visualisation. STAT automatically calculates from the specific requirement/criteria database tables “tbl_baseline”, “tbl_transparency”, “tbl_business_data”, “tbl_operational_data” through the value of evidence field: Conformance type (sum) Conformance Weight.

7.7.5 CSP Dashboard

This page enables the CSP to access STAT for carrying out essential tasks such as viewing and responding to checklists, uploading evidence, submitting a response to the checklist, receiving audit judgement from auditors and remedial actions that need to be implemented. The page uses a Hash MD5 security mechanism to run a session check and transmit a valid or invalid result.

Login/URL details:

Url: login1.php
Email: csp001@csp.com
Password: csp001

7.7.5.1 CSP Dashboard

This is the official landing page of the CSP when successfully logged in, and it comprises of the data display sheet with summed up figures of the CSP’s, the Auditors and the Audit checklist requirements. To the left are the menu options navigable to linked pages and with various tasks.

Dashboard Url: index.php

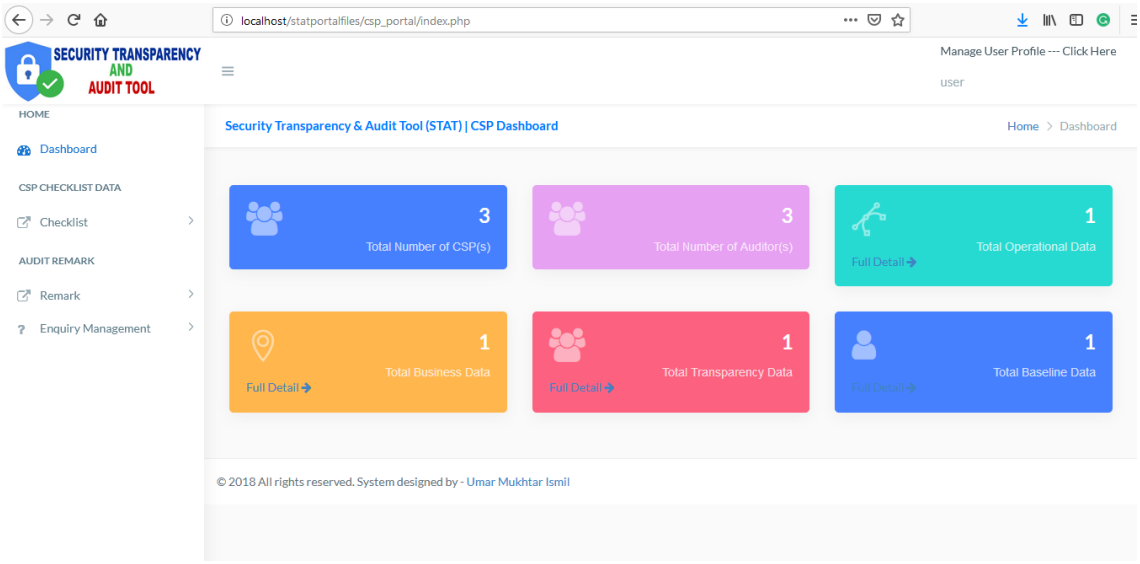

Figure 7.14: CSP Dashboard

7.7.5.2 CSP Checklist Options

This allows the CSP to select from the options for the available checklist i.e. Baseline, Transparency, Business and Operation to enable them to perform the task of viewing the requirements to be audited thereby responding to the checklist submitted by the Security Auditors with the accompanying evidence upload if required. The checklist data is stored and retrieved from database name "statportal_db" database tables "tbl_baseline", "tbl_transparency", "tbl_business_data", "tbl_operational_data". The requirement and its checklist also enable the CSP to view auditors submissions and take necessary actions on the checklist data types such as the "Target verification", "Base measurement", "Specification", "Question" and Evidence Upload. The checklist data types are expected to be returned responded to by the CSP for proper transparency.

Url: csp_baseline_response.php

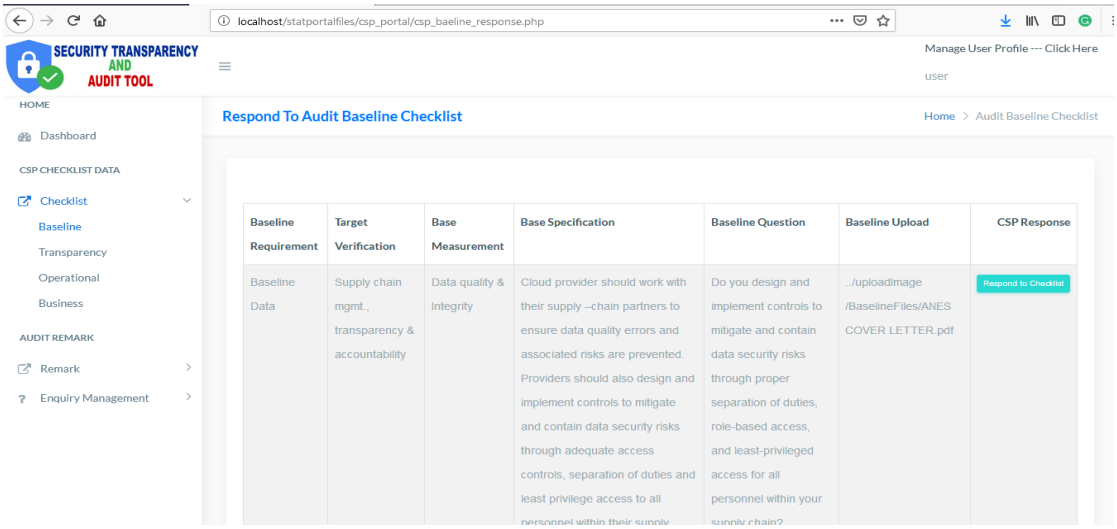

Figure 7.15: CSP Response to Baseline Checklists

7.6 STAT's Non-Functional Requirements

This section describes the tool's attributes that serve as essential considerations in the design of the tool for supporting critical functionalities. These include performance, security, reliability maintainability, portability and usability.

7.6.1 Performance

Performance is a crucial property of the tool. For the tool to run effectively, the HTML pages have to be able to update data on the database. The database, at a reasonable speed, must be able to supply requested pages to users. This is predicted to be highly processor-intensive and the database server must be deployed to keep up with all user requests.

7.6.2 Security

Security is one of the prime focuses of STAT, and as such, various aspects of security will be measures that will be implemented. From a basic security perspective, a combination of username and password are required to log into administrative and security auditor interface, while CSP interface is accessed using secure login details. Besides, STAT can hold data that represent generic information about the CSP's security practices and services, excluding sensitive or private data. As mentioned earlier, each feature is tied directly or indirectly to a user dashboard. Therefore, STAT uses the definitive users' access-rights to limit the scope of information or data accessible to each user. Each user is given a different feature-view to access data. To ensure adequate security, the implementation of STAT is designed to meet the following requirements:

- Each request to access CSP response and evidence must be authenticated to establish that an auditor is authorised to access the material that is requested.
- All communication between client interface that is accessed using a standard web browser and the server-side of STAT must be secured by a transport mechanism that offers confidentiality and integrity of data being exchanged.

7.7.3 Reliability

To ensure the reliability of the tool, a secondary backup database server will be implemented such that in case of a failure occurring to the primary server or incidents resulting to nonresponse, the secondary server will automatically start supporting the services. Also, a synchronisation mechanism will be used to ensure the synching of these two database servers. The possible solutions for synchronising these two databases include: establishing a full periodic backup for the entire database, or a trigger being created where all data on the main database are automatically copied to the secondary database.

7.6.4 Maintainability

The maintenance requirements of the tool should be very minimal because an initial configuration and implementation will be the only required system interaction. One area of user maintenance would be changed to administrative changes after the system is set up. Physical maintenance on

the tool's database server may be required, and this would result in a temporary loss of data and connectivity. Upgrades to hardware and software are predicted to have little or no effect on the tool but could result in downtime.

7.6.5 Portability

The tool is highly portable because once configured in a server, and it can be entirely moved to another server. The coding and program portability are possible between kernel-recompiled Linux distribution and Microsoft servers. However, for all the tool to work efficiently, all components must be compiled from source.

7.6.6 Reusability

The tool is designed such that the code is written in open-source programming languages and the components can be reused without having reusability issues.

7.7 Summary

In this chapter, the design and overview of STAT are presented. STAT is a specially designed tool that serves the role of supporting organisations to seek, collect and assess evidence from CSPs to establish how requirements are being fulfilled. The chapter provided the general description of the tool and the programming languages used in its development, such as PHP, HTML5, CSS and MySQL databases. It also presented design considerations, including the tool's architecture which is made up of three layers namely presentation, application and database layers. All these layers serve different roles. Also, the features of the tool are designed according to three crucial dashboards namely: administrative, security auditor and CSP dashboards. These dashboards provide numerous functionalities that are formed based on the audit activity in the proposed CSTF. Also, the workflow of the tool is presented, which illustrates how the tool is used from start to end, supported by screenshots of the dashboards for better illustration. Lastly, non-functional features that define the tool's attributes such as performance, security, usability, etc. are also discussed.

CHAPTER EIGHT

Implementation and Validity of CSTF

8.1 Introduction

The CSTF presented in this research is a proposed solution that aims to address the many issues associated with security transparency and trust-related issues. Implementation is a principal activity and one of the most critical steps in the development process, especially for a framework of significant importance like CSTF. The implementation aims at rigorously providing clear-cut assessment for demonstrating the ability of the research to produce the desired effect (Straub et al., 2004). It also comprises a set of associated methodologies and techniques to provide the means to establish the value, quality and relevance of research, and in some cases, offers essential feedback as a basis for improvement (Boudreau et al., 2001). Some methods and techniques could be adopted such as action research, descriptive, and experimental methods.

8.1.1 Empirical Research Method

An empirical research method is chosen for the research. Empirical studies are increasingly becoming popular in information systems research (Runeson and Höst, 2009). It has proven to be an effective research method to collect relevant data for investigating a specific problem in information systems. Therefore, the case-study approach was employed to serve as the implementation approach for this research, whereby two companies were selected based on accessibility through the researcher's contacts. A case-study approach is widely used in information systems research domain because it is useful for explanatory research projects, and serves as a basis for the development of well-structured research findings (Straub et al., 2004). The rationale behind employing a case-study is to obtain meaningful feedback regarding the validity and usefulness of CSTF as well as stakeholders view on the usefulness of STAT. Also, the author used questionnaires to collect feedback from stakeholders in the case-study contexts.

Two sets of questionnaires were prepared to form the guiding principles for collecting data. In particular, the first questionnaire aims at collecting stakeholders' perception and view about CSTF as a whole, while the second questionnaire is more specific to collecting stakeholder view about STAT in terms of its acceptability and validity to support security transparency. The questionnaires contain pre-formulated questions with defined response options. This consideration made the questionnaire highly relevant in obtaining feedback as the questions are clearly designed to help stakeholders express their view. Consequently, to efficiently collect feedback, it is imperative to develop the questionnaires using essential criteria that are formed according to established models for information systems adoption (Thong, 1999, Premkumar and Bhattacherjee, 2008). Specifically, these criteria are developed by considering Technology Acceptance Model (TAM) (Venkatesh et al., 2003) and Unified Theory of user Acceptance of Information Technology (UTAUT) proposed by Davis (Davis, 1989). The rationale behind these two models is that they are both widely used for assessing the organisation-level adoption of

various information systems products and services. Essentially, the criteria included ease of use/clarity, relevance, usefulness, flexibility and dynamics, compliance to security standards and best practices, trustworthiness (as shown in Appendix B and C).

8.1.2 Data Collection

At the initial stages of implementation, kick-off workshops were organised at each of the respective studied contexts. In each case, workshops were attended by senior management representatives and IT personnel with at least four years of working experience. The primary aim was to introduce the role of stakeholders in terms of the implementation exercises and feedback collection through the questionnaire. An overview of the process for CSTF and the essential features of STAT was introduced to help stakeholders develop an understanding of how the process/tool works, expected deliverables, procedures, and the methodology involved for data collection. Specifically, during the workshops, the process and implementation activities for CSTF were the focal point of presentation in case-study 1, whereas case-study 2 received more briefing on how to use STAT and its features.

Thus, a total of 35 printed versions of the questionnaires were distributed across the two organisations. The respondents were introduced to the aim of the project and how their feedbacks can contribute towards validating CSTF/STAT and the overall research findings. They were briefed about the criteria followed in formulating the questionnaire. Besides, the possible responses are designed to fit the purpose and can be indicated as either “I strongly agree”, “I agree”, “Not sure”, or “Disagree”.

Overall, a total of 31 questionnaires were returned by stakeholders from the two case-study contexts, implying a response rate of 88.5%. Table 8.1 provides a summary of the stakeholders that were involved and responses to the questionnaire within the studied case studies.

Table 8.1: Summary of Responses from researched case-studies.

Case-study	**Stakeholders that Participated**		**Stakeholders that Responded**	
	Senior Mgt.	IT Personnel	Senior Mgt.	IT Personnel
Case-study 1	5	13	4	12
Case-study 2	2	15	2	13
Total	7	28	6	31
	35		**31**	

8.1.3 Chapter Outline

The chapter is divided into four parts. The first part presents the overall implementation of the proposed CSTF, including the presentation of how data was collected and analysed. The case study is used to evaluate the implementation of CSTF from the first activity of the process through the last. This means that all the activities and steps involved have been applied to the case-study context, and stakeholders’ feedback is collected for analysis using six important criteria. The second part covers the implementation of STAT in the context of case-study 2. It includes the

application of the tool, as well as the collection of data for evaluating its usability and acceptability from stakeholder's perspective. The third part provides a comparison between this research and other related others found in the literature. The final part deals with the discussions on overall findings in respect to the implementation and validation of the proposed framework. Figure 8.1 shows an outline of the implementation approach for the proposed framework.

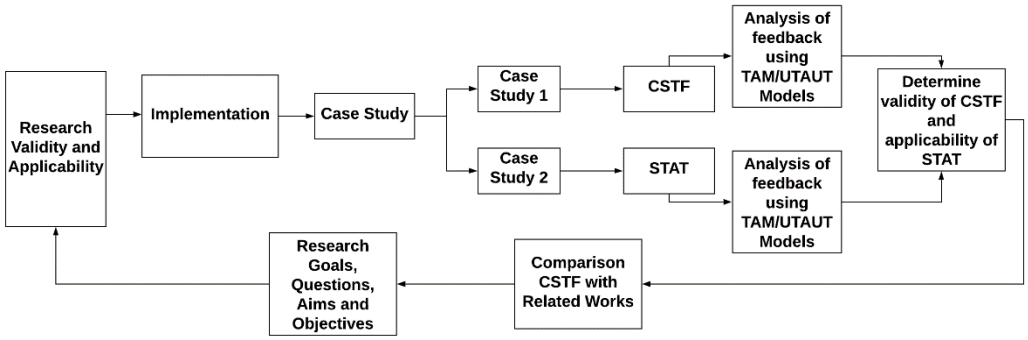

Figure 8.1: Evaluation Approach for the Proposed Framework

Part 1: Study 1 - Implementation of CSTF Process

This section presents the implementation of CSTF process using case-study 1. By following the cloud transition process from the start to completion over some time, we were able to comprehensively apply most of the activities and steps within the CSTF's process, as well as the opportunity to collect feedback towards evaluating its validity. Thus, a detailed description of the case-study is provided by firstly presenting background information and the existing system implementation, followed by the architecture for the migrated enterprise application. This is concluded by a practical demonstration of how the CSTF was achieved.

8.2 Company Background

The case-study is based on an anonymized company that specializes in property management in London. The company operates across multiple locations, with a total of 6 operational offices, five functional departments and a workforce of more than 100 employees. The company also has more than 2,000 properties under its management. The company uses an open-source enterprise content management (ECM) system that runs on PHP (server-side scripting language). ECM is generally a software that is designed to provide fundamental capabilities that allow users with limited or no technical expertise to create seamlessly, edit, review, categorize, index, and publish contents through user-friendly interfaces. The ECM facilitates the control, management, editing, and publishing of information and images on its website.

The company's staff worked with an ever-expanding document management solution (DMS), which is initially designed to complement their existing ECM software. The DMS is designed for capturing, archiving, indexing and retrieving data. It also enables the staff of the company to collaborate and manage the creation and flow of documents in a centralized repository, providing

solutions for gaining greater control of their business documents, information and processes. However, the computing resources of the company have been overburdened, leading to performance bottlenecks, in which the servers are slowing down to a crawl, thus slowing overall performance and affecting staff performance. The staff members found the system particularly frustrating and difficult to track, manage and store documents efficiently.

8.2.1 Candidate System for Migration to Cloud

To maximize solution effectiveness, increased efficiency and productivity, streamline services and achieve the highest degree of functionality to all users, the company has decided to outsource the DMS to the cloud. The company holds the opinion that outsourcing DMS to the cloud will address existing and potential challenges, as well as trigger the potential for more revenue and maintenance. Hence, the DMS has been designated as the candidate for cloud migration.

8.2.2 Existing Architecture of DMS

The current system is a web-based modular architecture that is built on Microsoft's supported products and is deployed on servers located in the data centre of the company. These include Windows Server 2003/2008 that serves as a document management server; Visual Studio for contents development; an SQL database that is used for storing and retrieving data. In particular, the system is implemented using.Net v.4 framework and other programming languages such as JavaScript for building many different frontend applications used by the company. In general, the DMS consists of four major components.

- ***Frontend***: consists of a web server that provides a web interface and is directly accessed and interacted with by users to utilize backend capabilities residing on the document management server. It runs on Windows Operating System (OS) and is built using ASP.NET. In other words, the frontend module is responsible for communicating with and transferring user request and device information to backend servers. Also, the frontend consists of end devices that are responsible for communicating with the application server.
- ***Backend***: comprises a Windows server and a MySQL database server. The Windows server provides essential services to users and performs other computation tasks such as user management, device management and document management. The database server stores personal information of landlords, tenants, and other sensitive information. The personal information, such as name and password, are used for authorization and authentication. Users interact with applications in frontend to make several forms of requests to the backend. The backend consists of:
    - User management module: this module is responsible for the management of users within the company, including user identification, preferences, and profiles.

It also enables user group and roles that facilitates sharing and collaboration amongst users, and allow manipulations of documents.

- Device management module: this is responsible for the management of authorized devices used by users. It stores information about the device name, type, status and other essential device characteristics.
- Document management module: this module provides three major functionalities for document management tasks such as document manipulation, synchronization and sharing. Document manipulation enables users to manage documents such as document creation, update, and deletion in addition to search, meta-data enriching and content preview. The Synchronization function enables cooperates with device agents to maintain data consistency between the document management server and user devices. The Share function enables document sharing among users, and it provides an efficient approach for users to share documents and facilitates collaboration among them.

- ***Database Server*** contains custom configuration and user-created files. It also provides shared storage for all system components and also responsible for keeping asynchronous communication between the frontend and backend. Electronic documents are also uploaded and stored in the database, where XML task files are created which describes an executable task for the backend. Generally, the database contains sensitive information about landlords, tenants, personnel, sales, marketing, finance, etc.

8.2.3 Deployment

The document management system is currently deployed on multiple servers that are hosted on-premise. Users from all branches of the company access the DMS and stored documents such as lease contracts, payments, landlord and tenant information etc. Once the cloud solutions are adopted, the company expects the CSP to allocate resources including virtual machines, networking, and virtual storage to achieve the required performance. On its part, the company will be responsible for installing and maintaining the Windows Server OS, .NET frontend applications, database and other components of DMS. The company believes that DMS can leverage the technological edge offered by cloud computing, including dynamicity, scalability and data replication. And being a small company, the management understands that expanding its infrastructure is not cost-effective.

8.2.4 Concerns for Cloud Adoption

The DMS handles a large volume of stored and real-time requests for documents creation, search and retrieval. If deployed in the cloud, the system must provide a consistent, transactional view of all user contents at all times, while also remaining dynamic for end-user needs. The company has some security transparency concerns regarding the adoption of cloud services. Firstly, it deals

with materials that require a high level of integrity and confidentiality, hence seriously concerned about potential issues relating to security and privacy, as well as the implementation and management of adequate security practices for securing the system by the CSP. Secondly, the management is particularly concerned about performance issues because all components of the system communicate over HTTP, which can be potentially harmful when storing and retrieving session data. Another concern is the conformance to specific security and other requirements of the system, such as integrity, trustworthiness, scalability, continuous availability of the system. The cloud is based on different technologies, security tools and practices that are generally difficult to monitor or measure. In general, the management of the company is concerned about whether the cloud offers sufficient transparency and whether it can sufficiently fulfil the company requirements.

8.3 Practical Implementation of CST for Study Context 1

As the company is considering the adoption of a cloud platform, we had the opportunity to follow the proposed process of CSTF to determine its relevance to a real-life context. As part of managing the entire implementation process, the company assigned a team of professional stakeholders to guide the execution of the whole implementation process, as well as ensuring necessary support to make sure implementation is achieved optimally. In this section, we provide a detailed description of how the CSTF was applied to case-study 1.

Before starting the activities, we indulged in a business rules discovery process that enabled a preliminary study of the company and its systems. During this time, a meeting was organised where the overall implementation plan is decided, a project team developed, and initial steps taken towards establishing the activities of the process. The project team comprises representatives from senior management, the IT department and other stakeholders within the company, all of whom have more than four years of experience.

The meeting commences with the project leader giving a brief presentation on CSTF, its aims, what the company can expect from the implementation, the role of participants, data collection approach, and a proposed meeting plan. The project leader also reiterated the company's responsibilities concerning providing necessary information and documentation about the assets, business process, as well as allocating human resources with suitable expertise to participate in the implementation process. Hence, the implementation process was performed through a series of organised meetings, workshops and discussions as presented below.

8.3.1 Activity 1: Stakeholder Analysis

We started the activities defined in the proposed CSTF with stakeholder analysis, which allowed the identification and understanding of key actors, their interests within the company and the roles that they can play. This enabled us to interact more effectively with key actors for gathering information and the implementation of CSTF. By conducting the stakeholder analysis, we were also able to identify and prevent potential misconceptions about the positions and roles played by

each stakeholder, identify sources of information regarding the organization and the cloud migration project.

8.3.1.1 Identified Actors

During the preliminary meeting and interaction with stakeholders, we have been able to identify the key actors that will support or influence the project and the different roles they play within the organization. This is mainly done by considering the context where the DMS is being used and how it will be hosted. We also considered actors from within and outside the company; thus, they were categorized according to internal and external actors. To present a comprehensive picture of actors, we have created an actor list showing actors and their roles. Each actor has a certain degree of activeness. Some actors fully participated in the CSTF implementation, while other actors are rather passive.

Table 8.2: List of Actors

Internal (Organisation)		**External**	
Actor	**Role**	**Actor**	**Role**
Senior Management representatives	Comprises high ranking personnel of the company whose responsibility is to coordinate, plan, oversee and direct the overall project.		
IT Managers	In charge of the company's technology strategy and responsible for coordinating and leading the IT experts/IT department of the company in implementing the process of the framework.		
System Analyst	Responsible for coordinating the development of systems, asset requirements, and control measures for ensuring the security of all assets.		
Security Auditor	Probes the safety and effectiveness of security controls and related security components of assets. Also, plans, execute and lead security audit, including evaluating the efficiency, effectiveness and compliance of business processes with organisation requirements, including generating a written report on audit findings.	**CSP**	Provides computing, storage, processing and related automated processes for hosting essential components of the document management system over the internet.
Content Manager	Responsible for approving content updates submitted by content editors and publishing all updates made to a document.		
System Administrator	Responsible for the technical oversight of the entire content management system. Also charged with installing, supporting and maintaining servers, responding to service outages and other problems.		
Content Editor	Responsible for handling day-to-day management and upkeep of contents, and optimisation of contents to meet business needs.		
Content Publisher	Responsible for releasing contents for use by other users.		
Registered users	Registered users those that have permission to use the system		
Security analyst	Responsible for identifying cyber threats and establishing plans and controls to		

	protect assets. Also responsible for performing vulnerability testing, risk analysis and security assessment activities		

8.3.2 Activity 2: Organizational Context

Through senior management support and active involvement, we embarked upon initial knowledge extraction and organizational context discovery activity where we gathered initial information which facilitated the identification of the business strategy within the company. This enabled us to gain an understanding about the way things are done in terms of the company's business process and the objectives to be achieved, followed by identifying the security goals that are part of an essential component of the company's assets. During this time, the present architecture of software systems and applications were reviewed, the architectural components are identified, and the high-level dependencies between them were established. We considered factors that influence its operations, such as the company's structure and the system and processes by which work is carried out. Based on the acquired knowledge, we established asset profiles consisting of security goals, criticality and the business process.

8.3.2.1 Assets Profile for DMS

To create a consistent asset profile, the IT manager was involved in explaining and documenting the system and its components, which provided the basis to identify assets and their security needs. The IT manager also presented a comprehensive overview of the DMS, which will be the target of analysis, from where we observed that the system comprises many different components. Based on these discussions, we analysed the architecture of the system intending to identify all dependencies, including how information is stored, processed and transported. By doing this, we were able to identify its assets, including data and applications. The asset profile is crucial because it can be utilized when developing and applying protection strategy, as well as risk mitigation plans for the system. We prepared an initial asset inventory of DMS together with details of the assets as shown in Table 8.3).

8.3.2.2 Security Goals of DMS Assets

After completing and agreeing on the asset inventory, the team turned its attention to identifying the security goals of DMS system. The security analyst conducted a high-level brainstorming exercise together with other team members to identify the most crucial security goals for the assets identified in the previous step. Security goals outline the qualities that an asset must aim to protect. At first, some representatives of the company emphasised that they are particularly concerned about the privacy of data held by the system. However, the security analyst explained that the team had reviewed the information collected during the previous step and examined every functional requirement. Hence, after a discussion, the project team decided to focus on the security goals of the system's known characteristics and security goals to include:

- **Confidentiality:** confidentiality goals are primarily intended to ensure that no unauthorised access to data, application and other assets is permitted, and that accidental disclosure is not possible. Information or data on all the system's components should be restricted to only those with the permission to access.
- **Integrity:** it must be ensured that data and applications of the DMS are safe from unauthorised modification and can be modified only by authorised users. It also provides the accuracy and completeness of records, and only authorised users should be allowed to modify contents.
- **Availability:** data and resources must be made available for authorised use without interference or obstruction. Data, application, and other system resources must be available when requested and easily accessible to authorised users.
- **Accountability:** The ability to trace activities or operations that occur to data, applications or system components to a particular source. All users must be accountable for the operations they have performed.
- **Conformance:** the system must operate as intended without any variation to expected behaviour, functions and regulatory requirements. The system must also be secured from vulnerabilities that can be exploited to cause unwanted behaviour.

8.3.2.3 Assets Criticality

Having identified assets of the system and associated security goals, the project team embarked on the next step of assigning criticality level to all the assets identified in the previous step. The criticality level is determined and assessed in greater detail as part of the asset profiling activity. Critical assets are those that are essential for supporting the DMS and the operations of the company. The security analyst determined the criticality of assets by applying a novel asset criticality system using fuzzy logic as proposed in the CSTF process.

8.3.2.4 Business Process

The business process identification and mapping workshop were organised to facilitate the discovery of business processes. The workshop brought together senior management from all units within the company to acquire valuable information from them in one instance. We set the context of the workshop and its objective communicated to capture the right information on how tasks are performed and executed within the company. The senior management provided a view of the process in their respective domains and leading questions were asked to understand the business process handovers from different units. Notes from all information from different unit managers were taken and provided a good view of the business process. These sessions served as a learning experience that revealed not only details about the business process, but also a business hierarchy, business rules, process operations and the assets required to support the business process.

Table 8.3 Asset Inventory

Asset ID	Asset Name	Asset Description	Business Process	Security Goals	Asset Criticality			Required Protection		
					Low Criticality	Moderately Critical	Highly Critical	Basic	Average	Significant
01	Document management server	Provides customers with the capability to create, store and manage documents and content electronically. The service incorporates digitization of existing documents and the means to manage information and data through workflow and process automation.	Assets and content management	Availability Integrity Authentication Conformance			*			*
02	Databases	Stores information about the company's customers, personnel, marketing, landlords, tenants, transactions, assets, finances, and other information about the company's business process.	Assets and content management	Integrity Confidentiality Availability Accountability Conformance			*			*
03	Company and customer data	Represent sensitive and private information about employees, tenants, landlords, finances, assets, etc.	Operations and services	Integrity Confidentiality Availability Conformance Accountability			*			*
04	Web & Application Servers	Provides, processes and delivers web contents such as images and assets information to employees and customers. The application server provides the platform for hosting frontend applications used by the company	Web contents managements	Availability Integrity		*			*	
05	Frontend Application	Provides the user interface that allows employees and customers to visualise, access, and patronise the company's services.	Service delivery	Availability Accountability Integrity		*			*	

8.3.3 Risk Management

The next activity involved a risk management process, whose goal is to identify as many potential threats, vulnerabilities and risks as possible. The activity was also organised as a workshop with inputs from actors with expertise on risk management. The actors involved in this activity included the security analyst, security auditor and members of senior management. Also, various methodologies and standards were employed at various steps of performing risk management. All participating actors were briefed about the parts of the standard/methodologies used and the benefit of doing so.

8.3.3.1 Threats Profile

The analysis team moved on to create a threat profile which contains the threats that can potentially affect assets and compromise sensitive information. To direct this process, the project's team members, a security analyst and system administrator were brought together to conduct an informed brainstorming session to identify a detailed list of threats. A list of security threats compiled by ENISA and CSA was presented to the team. Firstly, the team started with identifying a combined list of 10 security threats that they perceived to be important to the company's assets. After a brief reconsideration, the list was updated with two additional threats.

Secondly, the previously short-listed security threats had to be ranked. STRIDE and DREAD models were introduced to the participants to get an understanding and provide an approval of the methodologies that will be used for ranking the threats. STRIDE model was used to identify, and evaluate threats for determining whether tthreats threats fall under one of such categories as spoofing identity; tampering with data; reputation; information disclosure; denial of service; and elevation of privilege. In this regard, the team considered all potential threats from the perspective of hosting the DMS on-premise and in the cloud. Moreover, DREAD model is used for determining impact rating for the threats by asking the participants a set of questions according to damage potential, reproducibility, exploitability, affected users, and discoverability of threats. The adoption of these two models proved to be a simple, yet effective way to identify, categorise and determine the impact of potential threats, and it led to the participants having a better understanding of threat elements. It also mitigates any problem that may arise as a result of using simplistic threat categorisation and rating system, which are likely to be rejected by the team members. Thus, to document the threats associated with the assets, a template that shows several threat attributes is used. The security analyst documents the result of the meeting by filling a threat profile as shown in table 8.4

Table 8.4 Threat Profile

Threat ID	Threat Name	Description	Threat Category						Target Assets	Threat Severity					
			S	*T*	*R*	*I*	*D*	*E*		*D*	*R*	*E*	*A*	*D*	*Severity Rating*
T01	Data breach	Incidents involving unauthorised access, damage, alteration and disclosure of confidential data company data such as financial records, personal data for landlords and tenants, etc. A data breach can be the primary objective of a targeted attack or the result of human error, application vulnerabilities or poor security practices.				∗			Company and customer data	3	2	3	2	3	High
T02	Weak identity, credential and access management	The lack of scalable identity access management, weak multifactor authentication and lack of on-going automated rotation of cryptographic keys, passwords and certificates leading to data breach and system compromise.							Application and databases	2	3	3	2	3	High
T03	Insecure APIs	Malicious exploitation of application programming interface (APIs) and user interface (UI) that users use to interact with cloud services leading to the compromise of integrity, availability, confidentiality and accountability of user assets.		∗	∗	∗		∗	Frontend application	3	2	1	2	2	Medium
T04	System and application vulnerabilities	The exploitation of system vulnerabilities and bugs in programs to infiltrate cloud systems with the intent of stealing data, control or disrupting cloud service operations.	∗	∗	∗	∗	∗	∗	Application, database, company and customer data.	3	2	3	3	3	High
T06	Malicious insiders	Involve instances where current or former cloud employees, contractors, or third party service supplier who have authorised access to a cloud network, systems or data, intentionally misuse their privilege in a manner that negatively compromises the confidentiality, integrity or availability of an organisation's assets	∗	∗		∗			Application, databases, company and customer data.	3	2	3	2	1	Medium
T07	Advanced persistent threats (APIs)	Includes the application of sophisticated techniques using malware and cyberattacks that exploit vulnerabilities and infiltrates cloud systems to				∗		∗	All assets	3	1	1	3	1	Medium

		establish a foothold in computing infrastructure used by the organisation from which data and intellectual property are smuggled out.														
T08	Data loss	The compromise of valuable and sensitive data hosted in cloud infrastructure due to malicious attacks, theft, accidental deletion, or physical catastrophe such as an earthquake.			*		*		All data	2	2	1	2	1	Medium
T09	Insufficient due diligence	Insufficient exercise of due diligence before adopting cloud services to determine the risks and mitigation strategies put in place by the CSP and review the control	*	*	*	*	*	*	All assets	3	3	2	2	1	Medium
T10	Abuse and nefarious use of cloud services	Spammers, hackers and other criminals take advantage of the convenient registration, simple procedures and relatively anonymous access to cloud services to launch various attacks					*		All assets	2	1	1	3	2	Medium
T11	Denial of service	A malicious attack that focuses on shutting down cloud resources such as networks, applications, services and operating systems, making it inaccessible to legitimate users					*		All assets	2	1	1	2	1	Low
T12	Shared technology vulnerabilities	Misconfigurations, breaches and flaws in cloud resources, infrastructure, platforms and applications shared by users affect the organisation.				*		*	All assets	1	2	2	1	1	Low

8.3.3.2 Creation of a Risk Register

The analysis team had created a threat profile based on inputs from other participants, threat category and impact rating have now been approved. They have also developed the vocabulary needed to start identifying and assessing the risks that can impact assets. The analysis team embarked upon a series of structured workshops to identify risks, estimate likelihood, impact and control measures.

The first workshop entailed the identification of risks. The participants were presented with multiple sources of risks that are usually associated with cloud computing and assets of all types. Industry bodies provided the risk sources and they are regularly updated, which means that they offered up-to-date information about the most pressing security risks associated with assets hosted in the cloud. In particular, a list of risks provided by OWASP and ENISA was presented in the workshop, and the participants were tasked with selecting risks they perceive to be relevant. A combined list of 23 risks was identified but later narrowed down to 15 as shown in Table 8.5.

The second workshop was organised to enable the analysis team to estimate the likelihood and impact values of risks identified. During the workshop, all participants were engaged to provide an estimate that is as correct as possible. Hence, OWASP risk rating methodology was presented. The main idea behind using OWAS methods is that since the participants represent different expertise, they are likely to have a different opinion regarding the evaluation of risk likelihood and impact values.

Lastly, another workshop was organised to identify the necessary control measures for reducing or subdue risk. During this exercise, the analysis team was given a list of potential controls drafted by ENISA and CSC CIS. These controls provide a defence-in-depth set of best practices that are implementable to mitigate most forms of risks. Then, the analysis team was involved in a discussion to identify potential control measures and decided on which ones will control or reduce the risks to acceptable levels. Most of the control measures were taken from CSC CIS, while others were derived from ENISA especially in situations where CSC CIS have not provided controls for specific risks. Finally, a risk register was created showing the risks, likelihood, impact and control measures as shown in table 8.5

Table 8.5 Risk Register

Risk Name	Risk ID	Risk Likelihood				Impact to Security goals					Control Measures				Security Measures
		EoD	EoE	Aw	I_D	Conf.	Int.	Ava.	Acc.	Con	Fin.	RD	NC	PV	
Disruption of business process	R01	Med	High	Med	Low	-	-	Med	-	Med	Med	High	Low	-	Robust and effective implementation of data recovery capabilities, business continuity and disaster recovery plans, policies and processes that ensure the continuity of services in the face of disruptive events. Regular third-party audits to demonstrate adherence to standards, procedures and policies, and to establish the adequacy of restore procedures, including the accurate complete and timely recovery of business functions and services. Specific controls include: • Documented incident response procedures • Designated personnel to support incident handling • Running automated vulnerability scanning
Failure to provider security transparency and accountability by the CSP	R02	Med	High	Low	High	-	-	-	Med	Med	-	Med	Med	-	Regular and periodic performance of third-party audits to monitor CSPs compliance to security practices, effective implementation of proactive and reactive controls which should include data auditing, information tracking, log recording and supervising, hazard identification, and policy implementation. The CSP should ensure that all access and changes to the company's assets produce auditable trails or record that include clear indications of any delegations of identity or authorisation of all activities executed. Specific controls should include: • Publish information regarding reporting computer anomalies and incidents • Implementing automated monitoring and detection systems

															• Regular review of audit logs
Inability of the CSP to meet compliance needs of data and services	R03	Low	Low	High	Low	-	-	-	-	Med	-	Med	High		The CSP should be willing to undergo periodic security audits and present necessary security certifications that demonstrate compliance to relevant regulatory bodies. The CSP should also ensure meeting compliance obligations specific to specific laws and regulations within the UK, and all other laws and regulations formally documented in governance policies of the company such as ISO standards, Sarbanes Oxley Act, NIST Framework, COBIT, CSA STAR, and FEdRamp.
Inadequate data and application security, administration and control.	R04	High	Med	High	Low	Med	Med	-	-	Low	Med	High	Med	High	The existence of robust and effective security controls must be provided by the CSP, which provide assurance to the company regarding how data and applications are adequately secured against unauthorised access, change and destruction. A regular review and monitoring of user access must be performed, including the security administration of data and adequacy of rights, segregation duties, handling and disclosure of changes to asset status. Formal procedures should be implemented to prevent, detect and react to security breaches. Primary controls included are: • Establishing a penetration test program, and conducting regular external and internal penetration tests • Use of vulnerability scanning tools • Documenting penetration tests using open, machine readable standards. • Automated operating system patch management • Use of multifactor authentication for administrative access across all assets

Unavailability of critical data and assets	R05	High	Med	High	Low	-	-	High	-	-	High	High	Low	-	The CSP should provide significant guarantees against loss of critical data and services. Adequate back-up, recovery schemes, and data replication policies should be implemented by the CSP, which aim to prevent data loss, destruction and disruption of services. The CSP should provide proof the adequacy of restore procedures including accurate, complete and recovery of data. • Ensuring regular automated backups • Performing complete system backups • Testing data on backup media
Loss of data integrity and unauthorised changes to assets	R06	Med	Med	Low	Med	-	High	-	-	-	Low	Med	Low	low	Data segregation should be enforced using correctly defined through adequate and secure configuration of virtual machines and hypervisors hosting the system. All changes to assets should be managed in order to minimize the chances of malicious disruption, unauthorised changes and errors. Adequate control measures should be used including compliance to standards and policies, formal approval and acceptance of changes. The CSP must maintain sufficient audit logs that no unauthorised changes have occurred during a specified period. Controls included are: • Deploying system configuration management tools • Establishing secure configurations •
Data loss and leakage	R07	Med	Med	High	Low	High	Med	High	Low	Med	High	High	Med	High	Reactive and proactive security controls must be implemented to ensure the security and prevent unauthorised use, disclosure, damage or loss of data. Adequate back-up, recovery schemes, and data replication policies should be implemented by the CSP, which aim to prevent data loss, destruction and disruption of services. The CSP should

															provide proof the adequacy of restore procedures including accurate, complete and recovery of data. • Data encryption both in transit and at rest • Monitoring and detection of unauthorised usage • Maintaining an inventory of data • Enforcing access control • Ensuring regular automated data backups • Performing complete system backups
Failure to satisfy stipulated requirements by the CSP	R08	Med	Med	Low	Low	Med	Med	low	-	High	High	Low	Low	low	Periodic performance of audits and probing of CSP for establishing the fulfilment of requirements. The CSP must comply to standard, including Service Organisation Control (SOC)2, ISO 27001, NIST 899 and CSA

Where: *EoD = ease of discovery; EoE east of exploit; Aw = awareness; I_D = intrusion detection. Conf = confidentiality; Int. = integrity; Aav = availability; Acc = accountability; conf = conformance. Fin = financial; RD = reputation damage; RD = noncompliance; PV = privacy violation*

8.3.4 Activity 4: Requirements Specification

The next activity involves requirement specification, which was also organised as a workshop involving the risk management team members who decide and establish security controls from different perspectives that must be met by any potential CSP. During the seminar, the security analyst presented the risk register, while also reiterating the need to make a formal specification of requirements using existing risk control or develop a new compilation of security controls from CSA CCM. Thus, it was proposed that requirements be should be specified according to four fundamental categories, namely security transparency requirements, baseline security requirements, business requirements and operational security requirements. The participants became involved and based on their expert opinion; requirements are specified as shown in Table 8.6:

Table 8.6: Requirements Specification

Requirement	Control Domain)	Control Type	Control ID	Specification
Transparency	Supply chain mgmt., transparency & accountability	Data quality & Integrity	T1	CSP should work with their supply –chain partners to ensure data quality errors and associated risks are prevented. Providers should also design and implement controls to mitigate and contain data security risks through adequate access controls, separation of duties and least privilege access to all personnel within their supply chain.
		Incident reporting	T2	Information about security incidents that affected customers should be made available by the CSP through electronic methods such as portals.
		Provider Internal Assessments	T3	Internal security assessments should be performed at least annually to establish conformance and effectiveness of policies, procedures and supporting measures.
		Third-party agreement	T4	Supply chain agreements between the CSP and the organisation shall incorporate the scope of business relationship covered and the services offered; information security requirements; notification and/or pre-authorization of any changes controlled by the provider with customer impacts; timely notification of a security incident to customers; assessment and independent verification of compliance with agreement terms; expiration of the business relationship and treatment of customer.
		Third-party providers	T5	There should be reasonable information security across their supply chain, which includes all third-party providers upon which the CSP's information supply chain depends.
	Identity and access management	Audit tools access	T6	There should be appropriate restriction and segmentation access to, and use of audit tools that interact with the organisation's information systems to prevent compromise and misuse of log data?
		User access restriction/authorisation	T7	Policies and procedures should be established to ensure identities are only accessible based on rules of least privilege.
	Infrastructure & virtualisation Security	Audit detection	T8	A high level of assurance should be provided regarding the protection, retention and policy management of audit logs that adhere to applicable legal, statutory, and regulatory compliance obligations. User access accountability should also be provided for detecting potential suspicious behaviours and file integrity anomalies and supporting forensic investigations in the event of a security breach.
	Audit assurance & compliance	Independent audits	T9	Intended reviews and assessments should be performed to support the organisation address nonconformities of established requirements, standards, policies, procedures and compliance obligations.
	Application & interface security	Customer access requirements	T10	Security, contractual and regulatory requirements for the organisation should be addressed prior to granting access to an organisation's assets.

Baseline requirements	Datacentre security	Controlled access points	B1	There must be a classification of assets according to business criticality, service-level expectations, and operational continuity requirements of the organisation. A complete inventory of business-critical assets located geographical locations must be maintained and regularly updated, with defined roles and responsibilities.
		Equipment identification	B2	Before granting access request, automated mechanisms should be used to identify connection request based on equipment location.
		Policy	B3	A safe environment must be provided in rooms and facilities that store sensitive assets by establishing strong policies and procedures, implemented business process.
		User access	B4	Physical access to facilities storing critical assets must be restricted and controlled.
	Encryption & key mgmt.	Key generation	B5	Policies and procedures for managing cryptographic keys in the cloud service cryptosystem must be established.
		Storage and access	B6	Appropriate platform and data encryption validated formats and standard algorithms should be implemented while making sure that keys are not stored in the cloud but maintained by a trusted vital management provider.
	Identity & access management	Diagnostic configuration ports access	B7	User access to diagnostic and configuration ports shall be restricted to authorised individuals and applications.
		User ID Credentials	B8	User accounts credentials should be restricted in line with appropriate identity entitlement, and access management and according to established policies and procedures
		Source code access restriction	B9	Access to applications, programs, object source, and other forms of intellectual property belonging to the organisation should be restricted by following the rules of least privilege based on job function as per established user access policies and procedures of the organisation.
		Utility program access	B10	All utility programs that could potentially override system, object, network, virtual machines and applications should be restricted
	Human resources	Asset returns	B11	Policies and procedures should be established that ensure organizationally-owned assets are returned within an established period upon the termination or expiration of cloud service contract.
Business	Business community mgmt. & operational resilience	Business continuity planning	BS1	Procedures and policies shall be established for a unified framework that documents and ensures business continuity plans ensures business continuity plan are consistent in addressing priorities for testing, maintenance and development according to organisation's requirements.
		Business continuity testing	BS2	There should be planned testing of Implemented business continuity and security incident response plans on regular intervals or upon significant changes to CSP's environmental factors.

		Resource provisioning	BS3	Cloud resources should be sufficiently provisioned according to organisation's requirements.
	Identity & Access Management	Third-Party Access	BS4	A risk management assessment should be used to identify, assess and prioritise risks posed by business processes requiring third-party access to the organisation's assets. Followed by a coordinated application of resources to minimize, monitor and measure the likelihood and impact of unauthorised access to assets.
	Security incident management, e-discovery, & cloud forensics	Incident Response Legal Preparation	BS5	Appropriate forensic procedures and processes, including chain of custody should be maintained for the presentation of evidence to support potential legal action subject to relevant jurisdiction after a security incident. An organisation and other external parties impacted should be allowed to participate as per statutory requirements of forensic investigation.
	Governance and Risk Management	Baseline Requirement	BS6	Baseline security requirements that comply with applicable legal, statutory, and regulatory compliance should be established for organizationally-owned assets. Any deviation following change management policies and procedures must be authorised. Compliance with security baseline requirements should be periodically reassessed
Operational	Threat and vulnerability management	Antivirus/malicious software	OP1	Technical measures, including policies and procedures, should be established to prevent the execution of malware on organizationally-owned assets
		Vulnerability/patch management	OP2	Technical measures, policies and procedures should be implemented and established to enable timely detection of vulnerabilities within organizationally-owned assets to ensure the efficiency of security controls. A remediation approach for mitigating vulnerabilities should also be used. The CSP should inform the organisation of policies and procedures and identified weaknesses especially if the organisation is affected by emerging vulnerabilities.
	Governance and risk management	Risk assessments	OP3	Risk assessments associated with data governance requirements shall be conducted at planned intervals and consider: the awareness of where sensitive data is stored and transmitted. Compliance with defined retention periods and end-of-life disposal requirements; data classification and protection from unauthorised use and access.
	Datacentre security	Data centre security and asset management	OP4	Processes, procedures and controls should be implemented for ensuring physical security parameters for safeguarding sensitive assets.
	Application & Interface Security	Application Security	OP5	The provisions and recommendations of industry standards should be followed in the design, development, deployment and testing of applications and programming interfaces (APIs)

	Interoperability & Portability	APIs	OP6	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.
		Data request	OP7	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).
		Policy & Legal	OP8	Policies, procedures, and mutually-agreed-upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.
		Standardized Network Protocols	OP9	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.
		Virtualisation	OP10	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.
	Data Security & Information Lifecycle Management	Classification	OP11	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.
	Change Control & Configuration Management	Outsourced Development	OP12	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).

8.3.5 Activity 5: Assessing various CSPs

As the company is yet to adopt a specific CSP and migrate to the cloud, it becomes imperative to perform a comparative assessment of the security transparency services offered by various CSPs. The security transparency of CSPs elaborates the steps and actions taken towards fulfilling customer requirements and controlling security risks. A workshop was organised consisting of multiple team members. The team comprises representatives who have experience in the field of cloud computing, including system administrator, IT manager, and security analyst. They were briefed on the steps involved for collecting information, and the assessment questions and criteria that are used for determining suitable CSPs. The team then embarked on exploring commercially available CSPs that provide security transparency mechanisms for divulging information to existing and potential customers and subsequently performed the assessment. Hence, nine popular CSPs were initially identified for consideration but later reduced to four for the evaluation. The real names of the CSPs have been anonymized to conceal their real identity.

8.3.5.1 Collected Information

The assessment team used various channels and sources of information for discovering the extent of disclosure supported by the respective CSPs chosen for analysis. The focus is to establish how each of the CSPs can satisfy the requirements earlier specified in activity 5. Moreover, while all the CSPs support various forms of disclosing information, some have a greater depth of disclosure than others. Additionally, most of the CSPs have accessible public information published on their web portals, security whitepapers and reports, while other types of information are contained in a security audit reports that are shared with the assessment team after contacting the CSPs. However, information collected is not included in this thesis due to the size and nature of the information.

8.3.5.2 Performing the Assessment

The team proceeded to perform the assessment based on the information collected and using questions that are formulated according to the principles of security transparency, as presented in Chapter Four. A measurement metric is also applied, which uses a ‘Yes’ or ‘No’ for assigning score value to each question. If the answer to a question is ‘Yes’, then a value of 1 is assigned, meaning that the CSP has achieved an aspect of security transparency relating to that question. A ‘No’ answer attracts a value of 0 which implies the CSP does not meet the respective principle of security transparency in that regard. Measurement criteria that reflect the deployment practices of security transparency (i.e. opaque and explicit transparency) are applied for determining the type of security transparency proffered by each CSP.

From the assessment shown in table 8.7, it is discovered that all four CSPs have achieved explicit security transparency. CSP A scored 5, CSP B scored 7, while CSP C and D scored 6 respectively.

However, it is observed that CSP B gained the highest score of 7, which justifies the perception that CSP B has a higher degree of transparency than the others.

Further, the top management decided to migrate the DMS to the cloud and consolidate existing services to a centralised infrastructure-as-a-service solution that is hosted and maintained by CSP B. The IaaS incorporates necessary technologies that all work together to host the assets of the DMS. This implied that the IT systems in 6 locations of the company's offices have been merged into a unified system that is hosted and maintained by the CSP. Also, all data and applications have been consolidated and all locations now work seamlessly together in the same cloud service environment. A testing process was performed to check all applications that have been migrated are working correctly; confirm that all data have been migrated successfully; ensure all company and business data have been migrated and consolidated successfully, and ensure all peripherals in both locations are installed and configured correctly.

Moreover, during the transition to cloud services provided by CSP B, a Service Level Agreement (SLA) was signed, which is a contractual agreement that is composed of many clauses that describe the responsibilities of the company and obligations of the CSP in implementing security mechanisms, ensuring their effectiveness, and ensuring fulfilment of the set of specific requirement earlier specified. Another vital part of the agreement explicitly underlined a right-to-audit clause that stipulates the need for an independent assessment to be conducted at quarterly intervals by an auditor assigned by the company to ensure the security and privacy of assets, and compliance to requirements, which must be supported by the CSP with the provision of necessary evidences that are required as part of the audit. The agreement also covers the use of STAT as a supporting for conducting the assessment. The tool's features were elaborately described to the CSP including how it can be used for providing evidence and the procedure for implementing remedial actions. In general, the agreement covered all aspects of the processes involved in the use of STAT and the CSP obliged to support its use. Training regarding the use of STAT was given to a customer representative assigned by the CSP, including their role and how all features for CSP dashboard can be executed.

Table 8.7: CSP Assessment

Security Transparency Principle	Relevant Question	CSPs Assessed			
		CSP A	CSP B	CSP C.	CSP D
Availability	Does the CSP publish information relating to their security practices, policies and procedures as well as the status of customer assets being hosted in its cloud platform?	1	1	1	1
Clarity	Does the CSP publish information relating to security practices and procedures that is clear, precise, unambiguous, and which can be objectively interpreted by customers?	0	1	1	1
Current	Does the CSP publish up-to-date information regarding any changes to customer assets, policies, procedures, practices or current trends that might compromise customer assets?	0	1	1	0
Relevance	Does the CSP publish information that is relevant to the context of customer assets in terms of satisfying security requirements and addressing risks?	1	1	1	1

Notification	Does the provider support tools, features or services for timely reporting of unauthorised activities, incidents, operations, or processes that might affect or that affected customer assets?	1	1	1	1
Verifiable	Does the CSP support features and components that generate system and activity logs as evidence for tracing and verifying operational events of systems hosting customer assets?	1	1	0	1
Free/Low cost	Does the CSP publish information relating to policies, procedures and activities at a low cost or free of charge?	1	1	1	1
	Total	**5**	**7**	**6**	**6**
	Transparency Type	Expl icit	Expl icit	Explic it	Expl icit

8.3.6 Activity 6: Security Audit

The first step in the audit process is confirming with the top management when the audit will take place, which also provides an insight as to how often the cloud services will be audited. Three months after the successful migration, an audit team is created and assigned the responsibility to perform to evaluate the CSP's services and establish whether security processes and controls are being implemented according to the company's requirements. The team is headed by the Cloud Auditor and comprises other team members from senior management and IT departments who supervise the activities to ensure the audit is performed according to ISO/IEC 19011:2018 and ISAE 3402 Audit Standards. The audit activity requires the auditor to gather the necessary evidence to evaluate the compliance of the CSP and prepare a report of findings, including remedial actions.

In this regard, a workshop was organised and the steps involved in the audit activity are introduced to the participants. They are briefed about the features of STAT, shown how a security checklist is created and used; how evidence is collected; how to audit criteria are formed; how to determine conformance level; how audit findings are established; and how a report is generated. STAT was successfully installed, configured and deployed to support the audit activity.

8.3.6.1 Requirements to be Audited

A meeting was organised for the security audit team to review the requirements specified during the requirements specification activity to verify and establish what will be assessed during the audit process. After reviewing the list of requirements, it was agreed that the same four main categories of requirements (transparency, baseline, business and operational) and the associated control domains earlier prescribed should form the basis of the security audit. The summary of requirements, including the control domain and control types, are shown in Table 8.6.

8.3.6.2 Collection of Audit Evidence

The first phase of the assessment focuses on gathering, analysing and assessing evidence about the company's requirements. After verifying and documenting the requirements to be audited, the security auditor embarked on developing a comprehensive audit checklist that is key for carrying out the security audit and collection of evidence. As part of creating the checklist, the documentation of CAIQ and CIS are extensively studied and reviewed by the audit team to ensure

that it is adapted to the requirements of the company and that it does not become too generic. Therefore, the checklist was created, comprising a set of questions derived from CAIQ and CIS as shown in Appendix A. The purpose of the checklist is to provide the main focus and scope of the audit. Each question is associated with a type of evidence that is produced by the CSP as a direct response to the checklist, and which are appropriate to the requirements for which they are produced. This provided the benefit of obtaining different forms of evidence to support the audit process. The checklist was electronically inputted into STAT with the aim of using it to support the audit activity.

8.3.6.3 Performance of the Security Audit

Having received a response to the checklist and evidence from the CSP, the audit team evaluated all 133 questions in the checklist that fall under 17 control domains (target verification) and 32 (base measure) control types within the four key requirements. Essentially, the evaluation is performed on ISA 200 and ISA 402 Audit Standards using criteria the audit criteria, with the aim of subjectively determining a compliance level that is associated with it.

8.3.6.3.1 Step Conformance Levels

After the performance of the security audit and assessment of evidence, the audit team embarked on establishing the conformance level of the CSP in order to ensure that findings are coherently presented to top management. In all areas of the 4 requirements, the audit team determined conformance levels ranging from “very high” to “nonconformity”. A summary of the conformance levels according to each requirement as well as the overall conformance levels discovered by the auditors are provided. As the purpose of the analysis at this juncture was to provide the management with a snapshot of the CSPs conformance levels against requirements, no remedial actions are included in association with the conformance levels. A summary of the findings is provided as:

- 58% of requirements assessed were found to be very high conformance
- 7% of requirements assessed were found to be high conformance
- 18% requirements assessed were found to be medium conformance
- 5% of requirements assessed were found to be low conformance
- 12% of requirements assessed were found to be conformance

In addition, Figure 8.2 provides a summary of the overall compliance levels for all the requirements that have been assessed. To provide a more detailed picture, the compliance level for each requirement is provided, including a summary of questions and CSP responses, the count and percentage of compliance for each requirement.

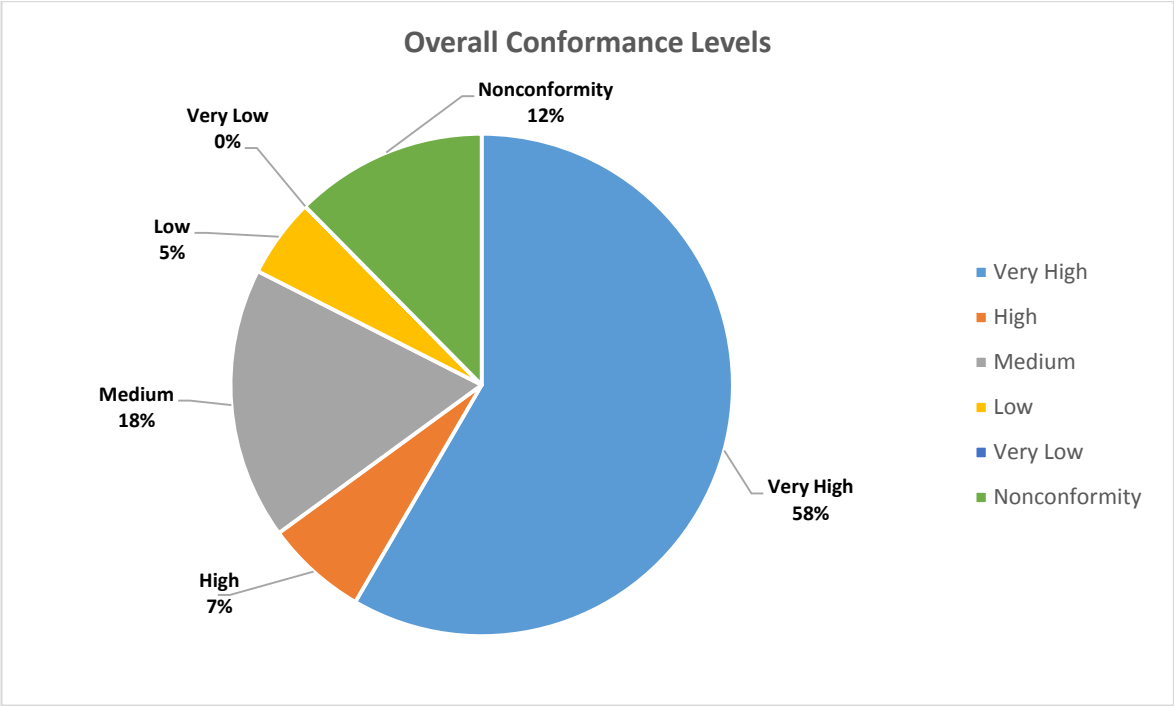

Figure 8.2: Summary of Overall Conformance Levels

9.3.6.3.2 Conformance Level for Transparency Requirements

The assessment results revealed that 40 questions in the checklist are related to transparency requirements and all questions have been responded to and evidence supplied. Also, the result shows that the CSP scored 64% "Very High" conformance level, 11% "High" conformance, 19% "Medium" conformance, and 6% "Low" conformance level. Details of the compliance level for security transparency are provided in Fig. 8.3

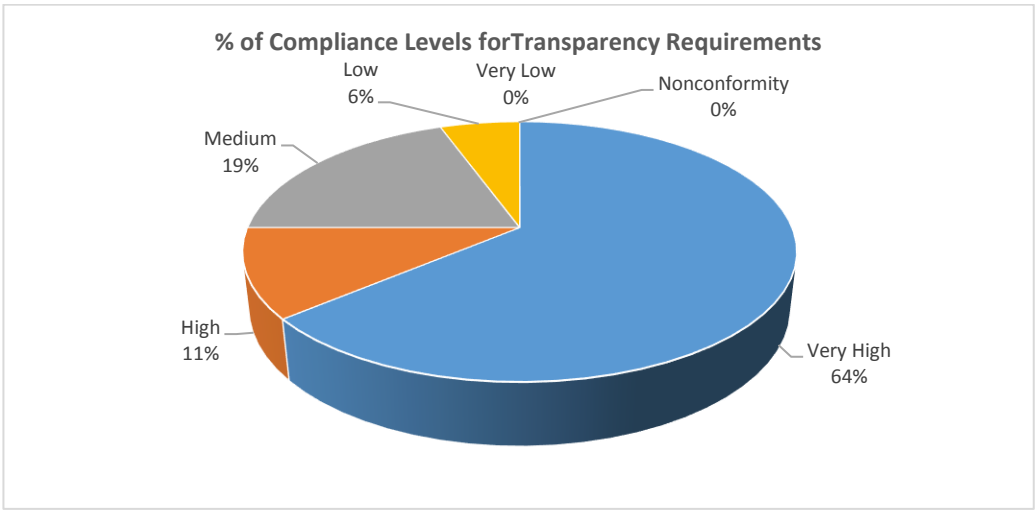

Figure 8.3: Transparency Requirement Compliance Levels in Percentage

8.3.6.3.3 Conformance Level for Baseline Requirements

The CSP scored 68% "Very High" conformance level. 10% "Medium" and 16% "Nonconformity" levels respectively as shown in Fig. 8.4

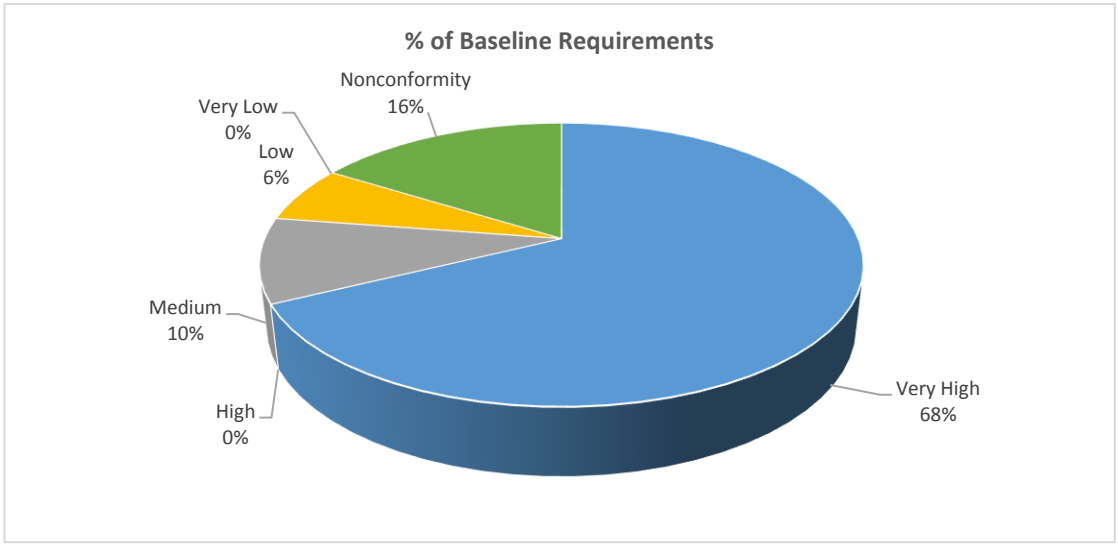

Figure 8.4: Transparency Requirement Baseline Levels in Percentage

8.3.6.4.4 Conformance Levels for Business Requirements

The summary of conformance levels for business requirements indicate that the provider scored 53% with "Very High", 17% with "High", and 10% with "Medium" conformance levels respectively, whereas 13% "nonconformity" is observed as shown in Fig. 8.5.

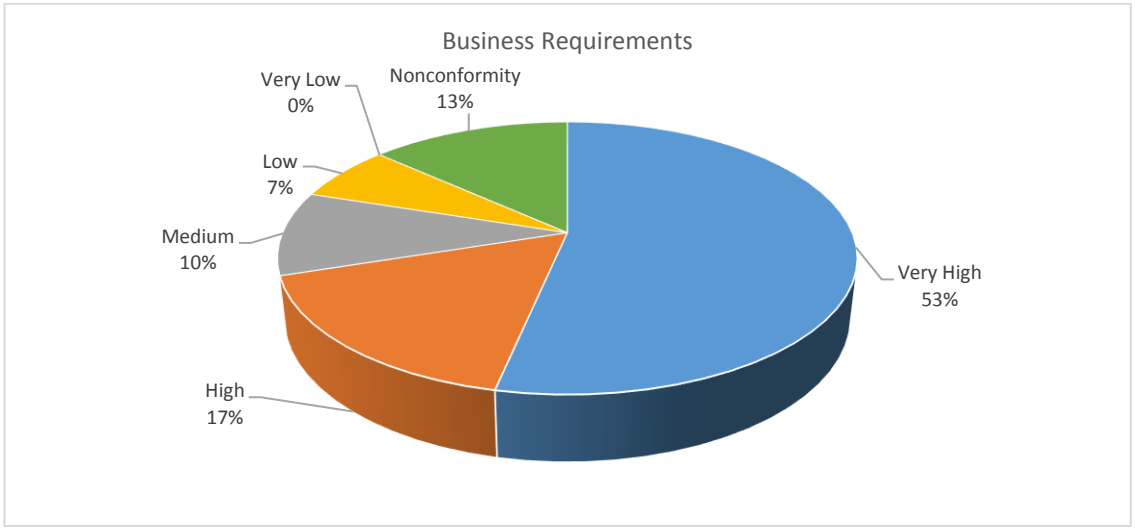

Figure 8.5 Count of Compliance Levels for Business Requirement

8.3.6.4.5 Conformance Levels for Operational Requirements

A summary of conformance levels for baseline requirements is provided. It indicates that this requirement has achieved significant non-conformance compared to the other requirements. 26% of the questions are non-conformant, while 65% scored "Very High", and 6% with "Medium" compliance level. These are shown in Fig. 8.6

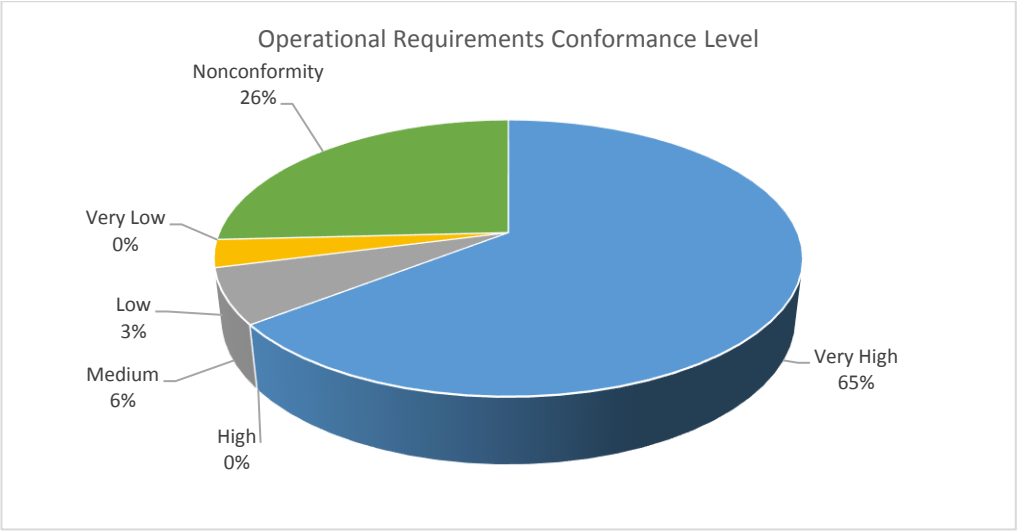

Figure 8.6: Transparency Requirement Operational Levels in Percentage

8.3.6.4 Audit Report

The security audit team had assessed and determined conformance level for each requirement. The majority of evidence provided by the cloud provided were assessed. The results of the assessed requirements led to the impression that some of the CSP security practices and mechanisms are somewhat robust from operational and technical perspectives, while certain areas must be reviewed and improved. Also, weaknesses were identified in some cases that contradict the company's requirements. The areas of requirements identified to have achieved low and nonconformity were thoroughly reviewed, prioritised and measured for their remediation were proposed by the audit team. Hence, based on the assessment undertaken, the result of the assessment was prepared which were documented and delivered in the form of an assessment report. The report contained a summary of findings on CSP conformance level and a detailed list of remedial actions that must be implemented by the CSP (as shown in Appendix D). The report was communicated with the CSP and an implementation plan outlining the duration it will take for each remedial action to be effected was also provided.

8.4 Analysis of Feedback Results for CSTF

This section presents an analysis of feedbacks collected from stakeholders through the implementation of CSTF. The focal point of the analysis is to determine the validity of CSTF in supporting organisations to achieve security transparency from the stakeholders' point of view. The total number of responses received is shown in Table 8.8

Table 8.8: Responses from received from Case-Study 1

Case-study	**Stakeholders that Participated**		**Stakeholders that Responded**	
	Senior Management	IT Personnel	Senior Management	IT Personnel
Case-study 1	5	13	4	12
Total	**18**		**16**	

The validity and acceptability results for CSTF and STAT are analysed based on the evaluation criteria (ease of use, relevance, usefulness, flexibility and dynamics, compliance to security standards and best practices, trustworthiness) as shown in Appendix A. The compiled results of responses from the stakeholders' according to the evaluation criteria are presented below.

8.4.1 Ease of Use Criteria

From the analysis result, 6 out of the 16 respondents representing 37.5% indicated they strongly agreed the proposed framework is simple to use, while nine respondents representing 56% agreed the framework is easy to follow. Only one respondent was not sure whether the framework is easy to follow or not. These results in a total of 93.5% expressing a positive opinion that the framework is simple and easy to use by organisations as depicted in Table 8.9.

Table 8.9: Stakeholders' Perception of **CSTF's** Ease of Use

Ease of Use		
Do you agree that CSTF is clear and easily understandable to intended users?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	6	37.5%
Agree	9	56%
Not sure	1	6.5%
Disagree	0	0%

8.4.2 Criteria

In terms of the relevance of the framework in supporting the attainment of security transparency, 37% percent of the respondents strongly agreed, and 50% agreed that the framework is relevant for helping organisations achieve security transparency. Further, 13% of the respondents are not sure about its relevance. These prove that the proposed framework is relevant for addressing security transparency related issues at the organizational level. This is shown in Table 8.10

Table 8.10: Framework's relevance for supporting the organisations achieve security transparency

Relevance		
Do you agree the proposed framework is relevant for supporting organisations to achieve security transparency?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	6	37%
Agree	8	50%
Not sure	2	13%
Disagree	0	0%

8.4.3 Usefulness Criteria

Based on responses about the usefulness of the framework in terms of producing expected deliverables, a significant increase in stakeholders' rating is observed. The responses show that 93% of the stakeholders agreed that the framework is useful for achieving expected results as shown in Table 8.11

Table 8.11: Responses on the Usefulness of CSTF

Usefulness		
Do you agree that the proposed framework is useful in terms of the expected deliverables?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	8	57%
Agree	5	36%
Not sure	1	7%
Disagree	0	0%

8.4.4 Flexibility Criteria

The proposed framework is designed with considerations to adapt to dynamic and changing environments. Based on the responses shown in Table 9.13, 27% of respondents strongly agreed that the framework is flexible, while 53% agreed that the framework on the framework's flexibility. The total percentile of those that agreed to represent 80%, which is significantly higher than those that are not sure (13%) or disagreed (7%) with the framework's flexibility as represented in Table 8.12

Table 8.12: Responses on the Flexibility of CSTF

Flexibility		
Do you agree the proposed framework is flexible to adapt to dynamic contexts?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	4	27%
Agree	8	53%
Not sure	2	13%
Disagree	1	7%

8.4.5 Compliance with Security Standards and Best Practices Criteria

The framework was developed on the foundations of various security standards and best practices. The acceptability rating of the framework's compliance with relevant laws and regulations achieved the highest rating with 94% of the respondents agreeing that it compliances with relevant laws and regulations, as shown in Table. 8.13

Table 8.13: Rating on Framework's compliance with relevant laws, standards and best practices.

Compliance with Security Standards and Best Practices		
Does the framework comply with relevant laws, standards and best practices?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	10	67%
Agree	4	27%
Not sure	1	6%
Disagree	0	0%

8.4.6 Trustworthiness Criteria

Trustworthiness is a holistic attribute that encompasses the ability of the framework to produce outputs according to users expectation. In this line, the trustworthiness rating of the framework achieved the lowest rating according to stakeholders' feedback. The acceptance rating shows that 74% of the respondents perceived CSTF as being trustworthy, whereas 3 respondents representing 20% were not sure about its trustworthiness. On the other hand, 1 respondent disagreed that the

framework is trustworthy. Based on rating results, it can be established that the framework's trustworthiness rating is validly significant. This is depicted in Table 8.14

Table 8.14: Responses on the Trustworthiness of CSTF

Trustworthiness		
Do you consider the proposed framework to be trustworthy in ensuring privacy and security?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	4	27%
Agree	8	46%
Not sure	3	20%
Disagree	1	7%

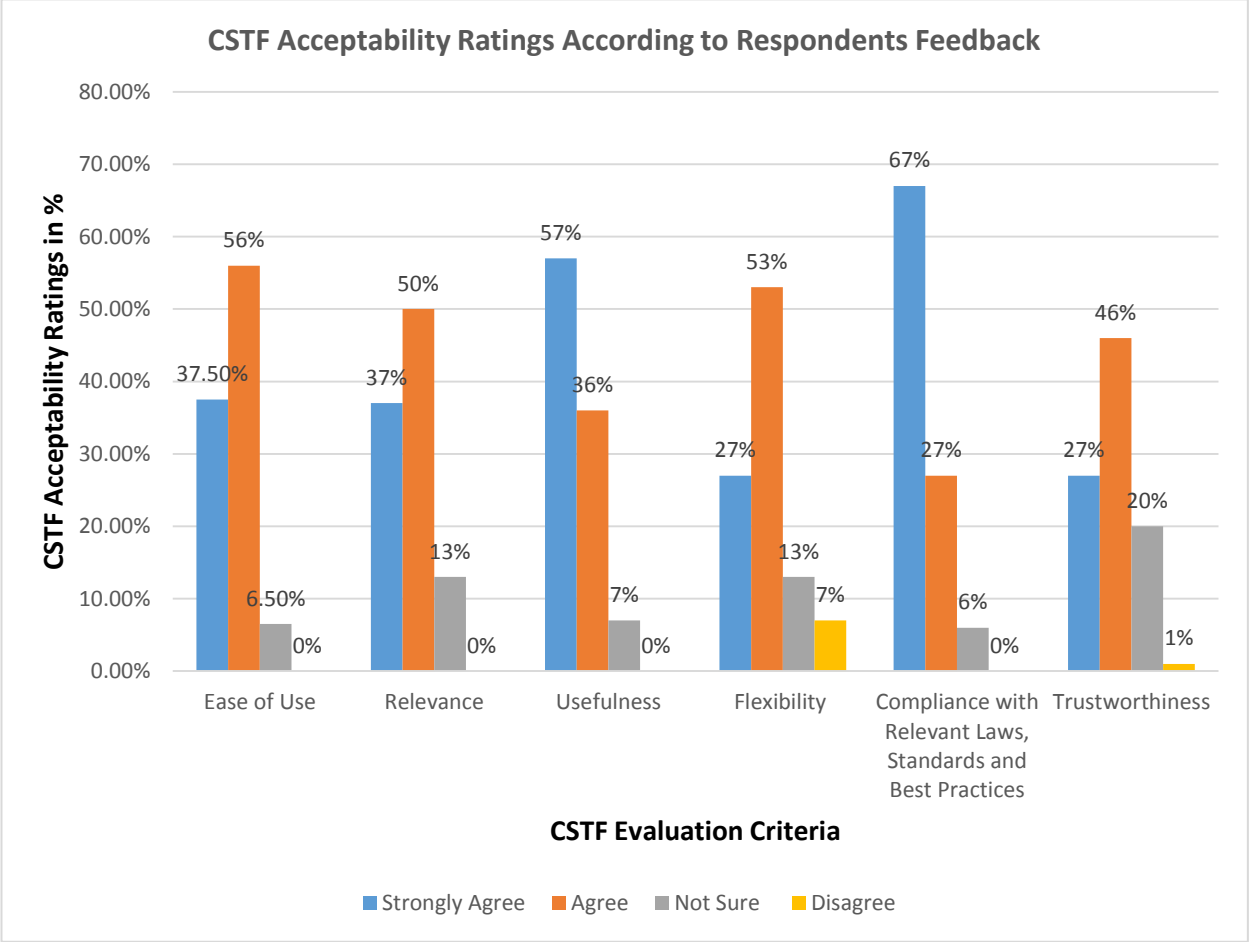

Figure 8.7: Acceptability ratings of the CSTF using six different evaluation criteria

8.5 Implementation Outcome and Lessons Learned: Case Study 1

An analysis of stakeholder feedback was conducted by following evaluation criteria derived from the renowned TAM and UTAUT models. The reason behind the analysis was to determine whether the proposed framework has achieved its intended aims for enabling and enhancing security transparency as proposed in the research objectives. The analysis results have shown positive outcomes in terms of the overall perception of stakeholders regarding the acceptability of CSTF. This assertion is made given the total positive responses obtained when "Strongly Agree" and "Agree" are combined to determine the optimism of respondents on each of the evaluation criteria, as highlighted below:

- Ease of use: 93.5% of the respondents considered the CSTF to be easy to use.
- Relevance: 87% of the respondents believed that CSTF is relevant
- Usefulness: 93% of the respondents believed that CSTF is useful
- Flexibility: 80% of the respondents considered CSTF to be flexible
- Compliance with relevant Laws, Standards and Best Practices: 94% of the respondents believed CSTF to be compliant
- Trustworthiness: 73% of the respondents considered CSTF to be trustworthy

Based on the overall summation of the feedback, as shown above, it can be established that an average of 87% of the respondents have accepted the proposed framework, while only about 13% views expressed otherwise. In a positive sense, the respondents have expressed enthusiasm and appreciation of CSTF for representing good coverage of their needs. They acknowledged that it had a positive impact on the organisations' security transparency aspirations. With this, it can be established that the research objective 1 and 2 have been achieved.

Also, through the process implementation, the researcher identified some valuable observations such as the importance of organisations using a simplistic approach that focuses on security transparency to guide their cloud strategies and adoption, rather than a generic strategy. The activities of CSTF are comprehensive, simple, and direct, which neither a required financial burden nor significant workforce burden to the organisation. Most of the activities within the process are easily implementable without the need for extensive training or instructions. The stakeholders that took part in the exercise were able to follow the steps without bottlenecks or major challenges. More importantly, the study observed that the incapacity to property identify requirements that focus on security transparency and adequately probe CSP internal practices are likely to result in major issues that cannot be rectified swiftly enough after cloud migration.

8.6 Case-study 2: Implementation of STAT

The previous case-study context mainly focused on the application of CSTF process – from the first activity through to the last. This case-study focuses and emphasises on the practical implementation of STAT in a company that is different from the previous one. The goal of the study is not to perform a repetitive application of the CSTF, a comparison of evaluation results or differentiate between the two case-studies. Instead, the focus is to evaluate STAT and determine its acceptance, applicability and validity to a real-life context. As such, the evaluation also helps to generalise the research findings on the overall approach of assisting organisations in achieving security transparency in the cloud.

The study context reflects a company that has already migrated its asset to the cloud, and whose major concern is to achieve security transparency. Hence, because cloud migration has already taken place, only the last activity of CSTF is followed, i.e. the audit activity which entails the application of STAT. Therefore, a description of the case study is provided, including and the

approach used for validity. Also, feedback from stakeholders is collected on the applicability and usability of the tool, which is presented in the subsequent parts of this Chapter.

8.7 Evaluation Approach

Similar to the first case study, an empirical method was selected to evaluate the main contributions of this study. Stakeholders are engaged and trained on the usability of the tool, including its features and functionalities in an introductory workshop. The stakeholders that took part are mostly employees with more than two years of working experience. The research team collected feedback data from the stakeholders on their general perception about the tool, according to questions that are formed in line with six important criteria: ease of use, relevance, usefulness, flexibility and dynamics, compliance to security standards and best practices, as well as trustworthiness. Data was collected through a questionnaire that was prepared and physically distributed using the six criteria. The questionnaire was filled by the stakeholders after the implementation exercise and returned to the research team. Subsequently, stakeholders' feedback are analysed to assess the participants' general perception and acceptance of the tool.

8.7.1 Company Background

As part of its strategy to improve and make it easier for the public to access urgent healthcare services, a Borough in London introduced a free healthcare system that gives patients and the public easy and swift access to urgent care, treatment and advice for less urgent medical problems, as well as providing clinical expertise, nurses and paramedics with an integrated access to patient's health information and assessment tool. All patients requests are made through a telephony system or alternative routes (online platforms) and received by a team of fully trained advisers, supported by experienced nurses and paramedics who ask questions to assess patients' symptoms, and give healthcare advice or referral to the local service that can help best. Also, the system also provides doctors with access to relevant aspects of patients' medical and care information, where the patient has consented to this being available. To this point, the Borough has a robust technical and organizational infrastructure in place that handles a million patient contacts and has also invested heavily in the telephony systems to support its strategic objectives. As a consequence of the high volume of care provided, the Borough recently migrated to a cloud-based environment that supports the clinical record system to improve patient care.

8.7.2 Technical Infrastructure

The system consists of a healthcare patient relationship manager (PRM) that manages the relationship between healthcare expertise and patients to foster effective communication, create a greater mutual understanding, trust and patient involvement in decision making. The system is a VOIP solution, which uses local intelligent queue servers and other essential databases to ensure complete flexibility of provisioning:

- *Summary Care Records (SCR):* This server hosts an electronic summary of key clinical information about patients. It is used by authorised healthcare professionals to support a patient's care and treatment. Patient's information is only stored and shared with the patient's consent, and additional information to the patient's record is added with a patient's consent.

- *Special Patient Notes (SPN):* The system provides a functionality that enables registered medical staff to access full medical record of patients, including special notes that can be attached to a new or existing patient to alert or highlight any specific care requirements, long term care plans or any other item of useful information for the patient.

- *Patient Demographic Service (PDS)*: A database that holds patients' demographic details such as name, address, and date of birth. It enables swift and accurate identification of patients by healthcare staff.

8.7.3 The Problem

Due to the sensitivity of personal health information (PHI) and stringent security requirements for the security, confidentiality and privacy of patients' information, the stakeholders are concerned about potential privacy and security, regulatory compliance, service reliability and interoperability issues that could arise as a result of migrating to the cloud. Specifically, the hospital's management is concerned about the prospects of being informed about where and how the PRM is managed, and the security controls applied in ensuring its protection. Also, the management is concerned about how the CSP is fulfilling essential security, transparency and operational requirements of the system. Thus, they agreed to use STAT in helping them to assess the CSP's activities and have full transparency on their assets.

8.8 Practical Implementation of STAT

In contrast to the previous case-study, the activities in this context primarily focused on the installation, testing and deployment of STAT for use by the company. The rationale behind this decision is the fact that the company has already migrated to the cloud, and the activity aimed to evaluate STAT. Therefore, the implementation exercises mainly involved stakeholder analysis, STAT deployment and collection feedbacks.

8.8.1 Stakeholder Analysis

The exercise started by identifying the stakeholders involved and keeping them informed about the tool, the activities, the installation preparations and a brief aim of the research. The actors are mostly personnel within the organisation who have at least three years of working experience. The identification enabled the research team to precisely engage stakeholders in the implementation and collection of feedback. Thus, the list of actors that participated in this context as shown in Table 8.13.

Table 8.13: List of Actors

Internal (Organisation)		External	
Actor	**Role**	**Actor**	**Role**
Representatives from top management	Charged with the responsibility of organising, directing, and controlling activities of the overall project for STAT implementation	**CSP**	Providing the platform, computing and storage facilities for hosting PRM
IT Managers	In charge of the Borough's technology strategy and responsible for coordinating and leading IT experts/IT department.		
Members of the IT Department	Different personnel within the IT department of the Borough that is charged with establishing, monitoring and maintaining information systems and services, including the administration and use of the PRM		
Security Auditor	Include expert personnel that are assigned the responsibility of conducting the audit by collecting, analysing and generating reports regarding the security and effectiveness of controls and overall safety of PRM components.		

8.8.2 STAT Deployment

A training workshop was organised, and stakeholders were given training for using STAT. During the training workshop, a demonstration was performed showing a practical guide on the installation and application of STAT, including the many dashboards that provide essential functionalities. Also, in a walkthrough conversation, a representative agent assigned by the CSP to support the company in performing the security audit was equally briefed about the steps involved and how to use STAT. The features of STAT are thoroughly explained with particular focus on the CSP dashboard that can be used by the representatives to accept audit invitation, answer the checklist and upload evidence where applicable, as well as receiving audit findings. Before the configuration of STAT, it was essential to ensure that the tool will behave as intended. The configuration possibilities were typically easy for the stakeholders to understand. The stakeholders are made to understand configuration settings in practice and what they should expect the system to do. After that, the STAT was deployed without many technical instructions as they already know and are familiar with the activity. Furthermore, STAT was comprehensively applied to serve its purpose.

8.9 Analysis of Feedback Results on the Validity of STAT

In this section, the analysis result of stakeholders' feedback regarding the effectiveness and usability of STAT are shown. The analysis is performed to determine the validity, relevance, and acceptability of STAT's features in supporting the organisation achieve security transparency from a technical perspective. Similarly, the analysis is performed according to the evaluation criteria earlier mentioned, which include: ease of use, relevance, usefulness, flexibility and dynamics, compliance to security standards and best practices, trustworthiness, as shown in Appendix B. Table 89.14 shows a summary of the responses to the questionnaire.

Table 8.14: Responses from received from Case-Study 1

Case-study	Stakeholders that Participated		Stakeholders that Responded	
	Senior Management	IT Personnel	Senior Management	IT Personnel
Case-study 1	2	15	2	13
Total	17		15	

8.9.1 Ease of Use Criteria

The ease of use criteria tends to measure the extent to which the tool can be used with ease and efficiency in terms of its functionalities and features. The result indicates that four respondents (27%) strongly agree and 9 (60%) respondents agree that the tool is easy to use, while two respondents representing 13% are not sure whether the tool is easy to use. This suggests that the tool has an overall acceptability rating of 87% as shown in Table 8.15

Table 8.15 Respondents perception about STAT's Ease of Use

Ease of Use		
Do you agree that STAT is simple and easy to use?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	4	27%
Agree	9	60%
Not sure	2	13%
Disagree	0	0%

8.9.2 Relevance Criteria

It is observed that a significant acceptance of the tool's relevance in supporting the attainment of security transparency. This assertion is manifested by the respondent's perception where 40% strongly agreed and 53% agreed about the tool's relevance. Only one respondent representing 7% disagree about the relevance of STAT, as depicted in Table 8.16

Table 8.16: Relevance of the tool in supporting the organisations achieve security transparency.

Relevance		
Do you agree that the tool supports the organisation in achieving security transparency?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	6	40%
Agree	8	53%
Not sure	0	0%
Disagree	1	7%

8.9.3 Usefulness Criteria

A significant number of respondents perceived the tool to be usefulness. From the analysis results, 57% strongly agreed, while 36% agreed to the usefulness of the tool. Only 7% are not sure, which indicates that the overall acceptability rating of the tool is this criterion is high at 93% as shown in Figure. 8.17.

Table 8.17: Responses on the Usefulness of STAT

Usefulness		
Do you agree that the proposed tool is useful in terms of achieving expected deliverables?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	5	57%
Agree	8	36%
Not sure	1	7%
Disagree	0	0%

8.9.4 Flexibility Criteria

The respondents are asked to express their view about the flexibility of the tool to adapt to dynamic contexts. From the responses analysed, there is a reduction in the acceptability rating of the tool's flexibility in comparison to other criteria. Thirteen percent (13%) of the respondents strongly agreed, and 67% agreed about the tool's flexibility. While 7% are not sure and 13% disagreed as represented in Table 8.18

Table 8.18: Responses on the Flexibility of STAT

Flexibility		
Do you agree STAT is flexible to adapt to dynamic contexts?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	2	13%
Agree	10	67%
Not sure	1	7%
Disagree	2	13%

8.9.5 Compliance with Security Standards and Best Practices Criteria

Regarding compliance with security standards and best practices, the respondents' acceptability rating shows that 33% strongly agreed about the tool's compliance with security standards, while 40% agreed and 27% expressed that they are not sure about the tool's compliance, which results to a total of 73% acceptance. This criterion achieved the lowest acceptability rating compared to the preceding ones as shown in Table 8.19

Table 8.19: Rating on STATs compliance with relevant laws, standards and best practices.

Compliance with Security Standards Best Practices		
Do you agree that the tool complies with relevant laws, standards and best practices?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	5	33%
Agree	6	40%
Not sure	4	27%
Disagree	0	0%

8.9.6 Trustworthiness Criteria

In comparison to other criteria, the trustworthiness criteria recorded a decrease in the acceptability rating from respondents. As observed from responses, 20% strongly agreed, and 47% agreed that the tool could be trustworthy in ensuring the security and privacy of data. Thirteen percent (13%) expressed doubts, while 20% are not sure about the tool's trustworthiness, as depicted in Table 8.20.

Table 8.20: Responses on the Trustworthiness of STAT

Trustworthiness		
Do you consider the proposed tool to be trustworthy in ensuring privacy and security?		
Response Options	**Response (Count)**	**Response (Percentage)**
Strongly agree	3	20%
Agree	7	47%
Not sure	3	20%
Disagree	2	13%

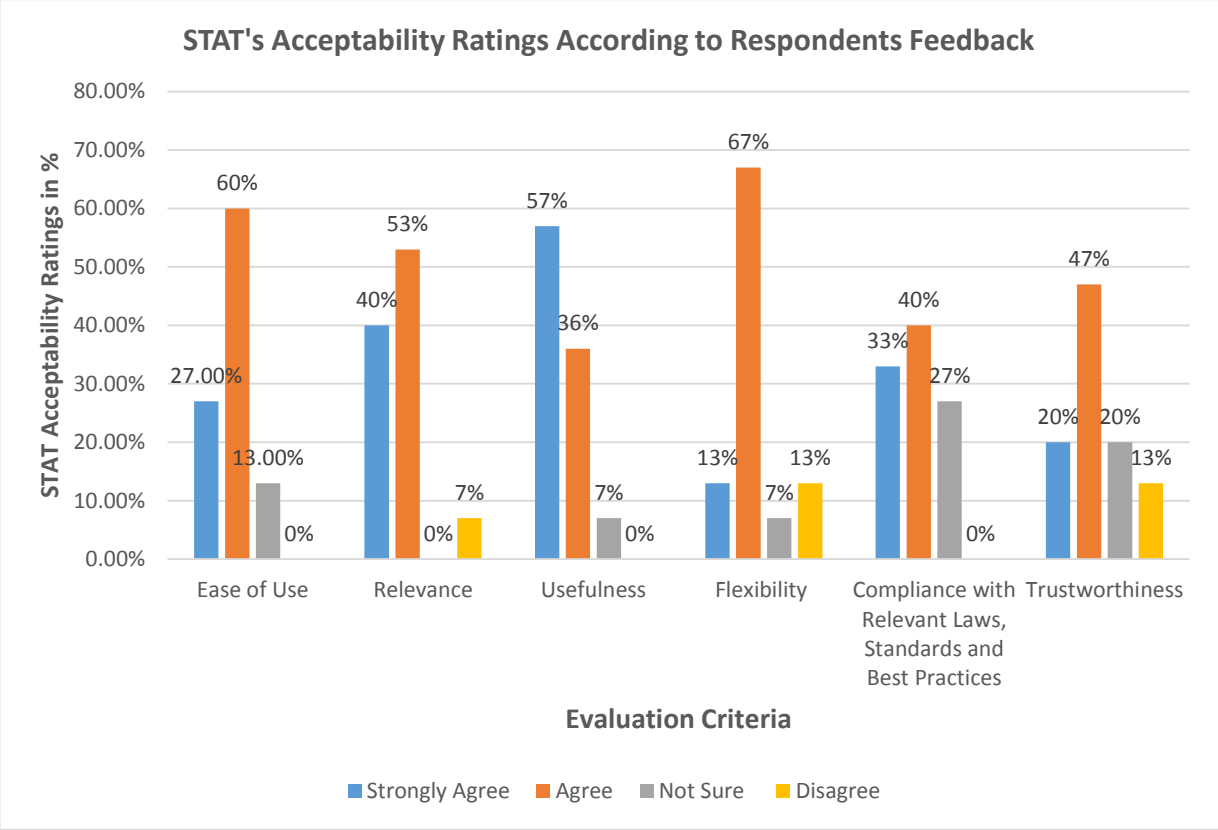

Figure 8.8: Acceptability ratings of the STAT using six different evaluation criteria

8.10 Evaluation Outcome and Lessons Learned: Case Study 2:

The analysis of respondents' feedback regarding STAT demonstrates significant acceptance rating of the tool. By computing all positive responses, i.e. "Strongly Agree" and "Agree", the evaluation outcome has revealed strong positive acceptability amongst respondents that have used the tool.

- Ease of use: 87% of the respondents believed that STAT is relatively easy to use
- Relevance: 93% think that STAT is relevant to the context
- Usefulness: 93% also considered STAT to be useful
- Flexibility: 80% believed that STAT is flexible
- Compliance with relevant Laws, Standards and Best Practices: 73% of the respondents believe that STAT is compliant with relevant laws and standards
- Trustworthiness: 67% perceived STAT to be trustworthy

An average of 82% of the stakeholders that evaluated STAT expressed optimism regarding the acceptability, validity and usefulness of STAT. The result is a reasonable one that highlights the significance of STAT to support the attainment of security transparency. The tool has enabled the organisation to address the key issues related to security transparency. In particular, the results have shown that STAT can be used as an independent security transparency tool or as a supplementary component to CSTF.

In general, STAT has proven to be highly useful and suitable for companies that have already migrated to the cloud. The implementation exercise was carefully observed, which enabled the researcher to document information that reflects on experiences. We observed that conducting an audit using STAT neither requires great resources, nor significant expertise. The assessment was run in a timely professional manner by auditors who were able to use effectively STAT in the context of the case study without significant hindrance. Besides, the time it takes to set up the system and train the stakeholders was relatively shorter than how the research team expected. The stakeholders were able to use the tool to achieve the audit objectives with effectiveness, efficiency and satisfaction. The features of the tool bolster the auditors' ability to assess because it provides quality features that facilitate the creation of an audit checklist, evaluation criteria and control actions.

8.11 Comparison between CSTF with other Works

This section provides a comparative analysis and discussion between this research and other study results found in the literature, particularly research results that enable security transparency in cloud computing. Such comparison aims to enable the researcher to generalise the research findings and identify the factors that reflect the context of security transparency.

To construct a comparison, some of the major scholarly works in the literature and industry projects that appear to address the issue of security transparency are selected to measure overall similarity and contrasting facets to CSTF. Further, several parameters comparison parameters in the form of questions are defined. The questions are formulated based on several distinctive contributions of the thesis, such as tool support; formal representation of knowledge; conceptualisation of security transparency; adoption of industry standards and best-practice; and implementation process for the approach.

8.11.1 Comparison Parameters

As mentioned earlier, the comparison parameters are created by formulating questions with respect to the key contributions of this thesis. Hence, the contribution is highlighted, followed by the associated question, and a brief description. The comparison parameters are shown in Table 8.21:

Table 8.21: Comparison Parameters

Parameter	Question	Details
Tool Support	*Does the literature provide tool support towards security transparency?*	Each approach is analysed based on the support of automated tool that augments and enhances security transparency from cloud users viewpoint through computation, analysis, visualisation, and evaluation of CSP conformity to requirement. Tool support is imperative for automated evidence collection from the CSP, and the verification and determination of CSP conformity to various requirement. Such a tool potentially strengthens security transparency specifically by making audit assessments and expert judgement procedure more effectively and timely. Thus, it is essential to have strong tool support, thereby facilitating and improving the effectiveness of security transparency (Robinson et al., 2010).
The conceptualisation of security transparency	*Does the literature establish and decompose the key concepts necessary for security transparency?*	It is paramount for each approach to dissect security transparency from cloud users' point of view by laying the foundational knowledge on key concepts. Ryoo (Ryoo et al., 2014) emphasised the need for an approach that identifies, analyse and represents security transparency from the lens of conceptual knowledge to enhance understanding and provide reference points to cloud users.
Formal representation of knowledge	*Has the literature considered the formal and explicit representation of security transparency using ontology?*	Ontology is regarded as an important technique for the formal and explicit specification of knowledge in the domain of interest and specifies how the concepts are related to each other through logical axioms expressed in a formal language. Youssef `(Youseff et al., 2008) the need for an ontology that ensures shared understanding of related by reducing conceptual vagueness and terminological confusion between cloud customers and users, supporting the reuse of knowledge, as well as supporting semantic visualisation.
Adoption of industry standards	*Does the literature leverage and integrate industry standards?*	Industry standards provide a significant level of assurance to customers that critical best practices are followed by cloud providers, as well as assurance that all operations are executed according to generally accepted security principle. This is due to the global acceptance of industry standards, best-practice, and frameworks (Lewis, 2013).
The comprehensive implementation process of the proposed approach	*Has the literature defined a comprehensive implementation process for the proposed approach?*	The implementation process is an important feature of every proposed approach. A process should provide a step-by-step actionable guideline for the implementation of the proposed conceptual model, framework or approach to cloud users to accomplish security transparency.

8.11.2 Comparison of Selected Literature against Comparison Parameters

In this section, the essential literature selected for comparison against the parameters listed in the previous section is presented, followed by the contrasting and similarity aspects with the work presented in this thesis.

- **P1:** Tool support.
- **P2:** Conceptualisation of security transparency
- **P3:** Formal representation of security transparency using ontology
- **P4** Adoption of industry standards
- **P5:** Comprehensive implementation process of the proposed approach

Table 8.22 Comparison of Selected Literature against Comparison Parameters

Literature	P1	P2	P3	P4	P5
CSA CCM (Cloud Security Alliance, 2017a)	x	x	x	✓	x
CSA CAIQ (Cloud Security Alliance, 2017b)	x	x	x	✓	x
STAR (Cloud Security Alliance, 2015)	x	x	x	✓	✓
Assurance Framework (European Network and Information Security Agency, 2010)	x	x	x	✓	✓
C.A.RE (Ouedraogo and Mouratidis, 2013)	✓	x	x	✓	✓
Nitro Web (Laurén and Leppänen, 2018)	✓	x	x	x	✓
HIDSCloud Deshpande (Deshpande et al., 2018)	x	x	x	x	x
Tian et al. (Tian et al., 2019)	x	x	x	x	x
CPTS (Pauley, 2010)	x	x	x	✓	✓
SMICloud Framework (Garg et al., 2013)	✓	x	x	x	✓
CloudHarmony (Leitner and Cito, 2016)	✓	x	x	✓	✓
CloudCMP Framework (Li et al., 2010)	✓	x	x	✓	✓
CSTF	✓	✓	✓	✓	✓

8.11.3 Discussion on Comparison Findings

The comparison in table 8.22 highlighted the results between CSTF and other security transparency approaches based on five important parameters that are peculiar to this research's contributions. The following section elaborates the comparison findings.

8.11.3.1 Tool Support:

In terms of tool support, there is substantial similarity, either fully or partially, amongst CSTF and those presented in the existing literature. For instance, (Garg et al., 2013) developed a SMICloud, which supports a decision-making tool that helps cloud customers to find the most suitable CSPs according to customers' key performance indicators and requirement such as quality of service, speed of VM, network latency. Customers provide their essential and non-essential requirement to the tool, which then generates a list of cloud services where the customer can deploy their asset. Also, CloudHarmony (Leitner and Cito, 2016) supports a performance measuring and analysis tool that run benchmark tests on multiple compute instances from different CSPs. The benchmark results could be used to compare the performance of CSP compute services using performance characteristics that are relevant to the customer, such as CPU and disk performance. CloudCmp (Li et al., 2010) also supports a benchmarking tool that compares the common services offered by various CSPs and uses the results to predict the performance and costs of customers asset when deployed on a CSPs environment. Hence, the most noticeable similarity between CSTF and the results in that literature is that they all support customers to specify the essential requirement that could be assessed. However, the difference between these works and CSTF is that they mainly focus on comparing multiple CSPs based on performance and cost characteristics before cloud adoption. CSTF supports the probing of CSP security

practices by seeking evidence about how CSP fulfils specific requirements, analysis of evidence, establishing assurances about the degree to which CSP conforms to such requirement, including the establishment remedial controls.

8.3.11.2 Conceptualisation of Security Transparency

The conceptual understanding of the factors relating to security transparency in cloud computing service is especially important because it provides simplification and consolidation of prior knowledge in the domain. The significant research efforts on security transparency have produced considerable propositions, and they all have different views and interpretation of security transparency concepts (Jaatun et al., 2018). The need for a consistent meaning and understanding of transparency is ever-increasing for helping organisations have a comprehensive understanding of how security transparency can be achieved and implemented from a customer perspective (Pearson and Benameur, 2010b). However, the results of the comparison have shown that existing literature have not considered the pressing need to define the various concepts that constitute security transparency. CSTF is unique in this regard because it conceptualised security transparency using a set of concepts. The concepts (such as actors, constraints, and goals) are based on Secure Tropos (Mouratidis and Giorgini, 2007). CSTF extends secure Tropos with new concepts such as evidence, risk, and audit in an attempt to develop the proposed framework. The reason for choosing Secure Tropos is that it provides an in-depth analysis of security issues from an organisation and its social setting. The concepts of Secure Tropos and those proposed in our approach are integrated to provide a comprehensive understanding of the salient aspects that constitute security transparency and how it could be achieved.

8.3.11.3 Formal Representation of Security Transparency using Ontology

It is worth mentioning that the comparison results have shown that existing literature commonly represented security transparency either by using natural language or graphical representations, both of which lack the computational semantics needed to enable automated validation or execution of key concepts. In some literature, the authors have mainly considered the technical aspects of security transparency but not it's related contextual and organizational aspects. In particular, contributions in the literature have not particularly used formal models to create a common language for describing the processes and functions associated with security transparency. CSTF has addressed the gap as mentioned earlier because it adopted an ontology approach, which is a formal language that can help in the detection of semantic ambiguities, uncertainties and contradictions between the concepts of security transparency. The ontology defines a structured set of security transparency concepts, the relationship between these concepts, and a set of rules on how the concepts can be combined to represent semantic knowledge. It also reduces the conceptual vagueness and terminological inconsistencies by providing a common understanding of related concepts between cloud customers and CSPs. The ontology is machine-

readable and the use of concepts and relationships ensures that knowledge is represented completely.

8.3.11.4 Adoption of Industry Standards

Industry standards generally provide well-documented rules, guidelines, or characteristics for activities, and consensus approved by a recognised body which aims at the achievement of the optimum degree of order (Saint-Germain, 2005). A significant number of the literature considered for comparison has promoted the use of industry standards to enable consistency and a reliable metric for assessing the validity of results. For example, CSA CCM and CAIQ (Cloud Security Alliance, 2017a) are both intensively mapped to various security standards such as NIST CSF (Shen, 2014) and CoBIT (Von Solms, 2005). Furthermore, the authors in CPTS (Pauley, 2010), C.A.RE (Ouedraogo and Mouratidis, 2013), (Leitner and Cito, 2016) and CloudCMP (Li et al., 2010) have also considered the integration of industry standards in their approach. Most of the standards used by these works are more security-oriented, which means that there is a significant similarity with CSTF in terms of the integration of security standards. However, CSTF uses a unified approach by focusing on specific sections of renowned guidelines, frameworks and models rather than just security standards. They are mostly applied across different activities within the process by looking at specific features within the standards, frameworks, models and guidelines and where they best fit into the process. For example, CIS CSC and ENISA have been used for identifying risk control measures. This is because CIS CSC provides 20 controls categorised into three prioritised and defence-in-depth best practices that are implementable to mitigate attacks against systems and networks. Some of these controls are relevant to cloud security transparency, while others are less relevant. Further, ENISA provides 27 baseline security controls that are more CSP-oriented and focuses on control measures that protect cloud computing systems against operational risks. As a result, a parallel matching is performed for identifying semantic equivalence between controls in CSC CIS and ENISA. Also, Microsoft has proposed a structured approach for analysing the security of systems and application, namely DREAD and STRIDE models. Such models enable the identification, classification, rating, comparison and prioritization of security risks associated with systems and applications, and these two important models have been adopted for threat analysis. OWASP methodology is also used for determining the impact of risks because it estimates risks from business process and technical perspectives, and it is highly adaptable and applicable to most organisations of all sizes. In identifying relevant risks, risk sources from ENISA and OWASP are also considered mainly because the latter maintains a regularly-updated list of most pressing cloud security concerns, and the former provided a list of 35 risks that fall under categories such as technical, organizational, legal and non-cloud specific. Besides, in the course of specifying requirements, CSA STAR is adopted because it provides sixteen essential security principles that serve as a guide to CSPs and also provides organisations with the structure to achieve asset security in the cloud-tailored

environment. In the audit activity, ISAE 3402 and ISO 19011:2018 is used mainly because it sets forth internationally accepted guidance on conducting and managing audit program that applies to all organisations that need to conduct security audits.

8.3.11.5 Implementation Process

An effective implementation guide for any approach to a problem has been highlighted as a crucial success factor for any proposed solution to an existing problem (Gottschalk, 1999). A process provides a systematic set of activities that aim to achieve desired objectives, deliver results and outputs (Chang et al., 2016). The various studies examined have such as Nitro Web (Laurén and Leppänen, 2018), SMI Cloud (Garg et al., 2013), CloudCMP (Li et al., 2010) and CloudHarmony (Leitner and Cito, 2016) have provided the underlying architectural and technical guide for implementation. ENISA's Assurance Framework (European Network and Information Security Agency, 2010) also developed a methodology based on a set of questions that organisations can ask a CSP to get the assurance that assets can be sufficiently protected. This shows that there is a commonality between the literature mentioned above and CSTF. However, the process proposed by CSTF is more transparency-oriented. It consists of different phases of activities that organisations can follow for understanding and strengthening security transparency by looking at important considerations such as identifying roles, assessing risks, etc. The process also guides organisations to build a cloud migration strategy from initiation to completion phases based on the need for continuous validation of CSP promises. Also, the process is guided by a variety of leading industry best practices, frameworks, guidelines and standards that are generally applicable to all organisations regardless of size. This implies that the process is all-encompassing in nature, not tailored to a specific organisation type or solution, but built upon high-level considerations to ensure important cloud adoption issues are not entirely missed.

8.12 Empirical Studies Conclusions

The empirical research method used in this research and the application of the case-study approach has allowed the researcher to perform an in-depth longitudinal examination of different real-world contexts. The adoption of the case-study technique has enabled the researcher to make systematic observations, collect and analyse data, and to establish findings within the context which activities took place. It also allowed the researcher to observe complexities of real-life situations, which may not otherwise be captured through other forms or methods. Many participants from two different companies - whose names have been anonymised for confidentiality reasons, took part in the implementation and determining the validity of the research. The participants provided invaluable feedback on their experiences and perception of the proposed framework and its supporting tool. The analysis of the participants' feedback provided an encouraging finding that shows the relevance, validity and acceptability of the proposed framework amongst organisations. The participants expressed optimism about CSTF

and its potentiality in addressing the current and emerging security transparency issues in cloud computing.

8.12 Chapter Summary

In this chapter, the empirical evaluation of CSTF and STAT was discussed. The chapter provided a detailed discussion regarding empirical studies for validating this research, using a case-study approach. Questionnaire technique enabled the collection feedback from participants that took part in the implementation of CSTF and STAT with the aim of analysis for establishing the validity, acceptability and relevance of the proposed framework. The chapter also presented results from the case-study contexts. Stakeholder feedback was collected and used to evaluate their perception and view of regarding the validity and acceptability of the framework. The stakeholders expressed confidence and reasonable satisfaction. The results proved that the proposed framework is highly relevant for helping organisations in attaining security transparency. Also, the chapter provided a comparison between some of the key approaches to security transparency in the literature. Five comparison parameters have been defined based on which CSTF could be compared against selected the selected literature. The comparison parameters are created according to the distinct features or contributions of CSTF. The results of the comparison have shown that the research has made notable contributions to the knowledge domain.

CHAPTER NINE

Conclusion and Further Research

9.1 Introduction

Cloud computing offers a combination of advantages such as agility and scalability that are driving businesses to rely on cloud technology as a foundation for enablement of business opportunities. It enables organisations to adopt innovations and respond to business demands quickly. But these advantages cannot be fully utilised if transparency into cloud environments is not improved. Cloud services that offer limited visibility result in significant security and operational challenges to organisations, such as the problems in attaining operational requirements, challenges reporting security issues to management, and other forms of compliance issues. Security transparency has a crucial role to play in the future of cloud services because it facilitates visibility and provides organisations with a view on the status of assets and how important requirements are satisfied. These considerations necessitate for transparency to be strengthened so that businesses can be poised and stimulated about cloud service adoption. Improved transparency will certainly revamp the level of trust between organisations and CSP, and ultimately shape the future of cloud adoption.

This thesis has proposed a solution for addressing security transparency-related challenges. To do so, CSTF has been proposed that supports organisations develop foundational knowledge of security transparency, integrate the concepts within organizational settings for guiding cloud migration, and a tool called STAT that helps the collection and assessment of evidences from CSP. The proposed CSTF and STAT have been validated amongst different real-environment study contexts. Furthermore, the feedback has been collected and analysed to establish the acceptability, usability, relevance and validity of the proposed framework.

To conclude this thesis, this is the final chapter that presents concluding remarks of the entire research. It expounds how the research objectives could be met, expatriate research contributions to knowledge, and highlights limitations and future research directions.

9.2 Responding to Research Questions and Objectives

The proposed CSTF has been developed and validated against real-environment case-studies to meet the research aim, which was to *develop a systematic framework that supports security transparency in cloud computing, which will ultimately increase businesses trust in cloud services*. To ensure that the research aims above are satisfied, three objectives were specified as:

- ***Objective 1:*** Develop a novel framework that aims to provide users with a solution to achieve security transparency from conceptual, organizational, and technical perspectives.

- *Objective 2:* Propose an implementable process for cloud migration activities which is founded on multifarious industry standards and frameworks to achieve security transparency.

- *Objective 3:* Develop a dedicated security transparency tool that enables organisations to continuously collect evidence, probe, and assess CSP's conformance to established requirements, as well as suggesting remedial actions in areas where security improvements are needed.

It became imperative that the three research objectives shown above are checked to ascertain whether they are accomplished in the course of the research. The research has strived to ensure they are accomplished, and an attempt has is made to justify how the objectives are accomplished

9.2.1 Develop a Novel Framework

A fundamental objective of the research entails the development of the proposed CSTF, which is also a requisite for achieving the final research aim. Objective One was accomplished via Chapter Four and Chapter Five. Chapter Four, on the one hand, provided the rudimental principles, background knowledge and understanding of cloud security transparency. Sections 4.2 – 4.5 introduced the basics of transparency from broad perspectives and different domains considered in forming a novel definition of the term from cloud context. Also, Section 4.4 provided the properties of security transparency in terms of the building blocks that are essential in delivering security transparency. Section 4.6 establishes the fundamental principles and norms that govern the delivery of transparency, which were borrowed from different domains and tailored to cloud security. Further, there are various circumstances where organisations can seek and receive information regarding CSP activities and services. Thus, in Section 4.6, the research elaborately outlined the types of situations or scenarios where CSP tend to supply information to stakeholders, such as proactive, reactive and contractual. This led to categorising security transparency according to proactive, reactive and contractual. Mostly some information disclosed by the CSP could be inconsequential to stakeholders or perhaps contradictory. Therefore, the two types of security transparency that can be associated with a CSP are defined in Section 4.8.

On the other hand, in Chapter Five, the proposed framework— as per considerations from the principles and background knowledge formed in Chapter Four was introduced and discussed. The Chapter started with the approach adopted for the proposed CSTF that uses three levels of abstraction. Each level is associated with certain deliverables. The first level establishes and provides an understanding of the various concepts that constitute security transparency, which is formed based on the principles of security transparency presented in Chapter Four. The second level deals with important concepts that are used within organizational setting to achieve security transparency. As it is a highly recommended and common practice to build any framework of relevance based on established theory or methodology, a novel agent-oriented software

methodology called Secure Tropos (Mouratidis and Giorgini, 2007) was chosen to develop these concepts. Secure Tropos covers software development from initial requirement analysis and uses concepts such as actors, constrains, and goals. The concepts in Secure Tropos are extended with new concepts such as evidences, and audit in an attempt to develop concepts at organizational level. In addition, ontology and semantic web modelling language were applied (Maedche and Staab, 2001) to broaden further and improve domain knowledge of concepts at organizational level. The last level covered the various technical means that can support the attainment of security transparency and highlighted some conventional mechanisms and initiatives. This enabled the adoption of a security audit as a means for achieving transparency.

9.2.2 Propose a Security Transparency Process

Objective 2 aimed at proposing an implementable security transparency process for cloud migration activities based on the framework, which is formed based on the principles of various industry standards. There are existing processes for cloud migration such as CloudGenius (Menzel and Ranjan, 2012), however, such processes have certain limitations because they are not specifically developed with focus or emphasizing on security transparency. In order to fulfil this objective and address the gap, the research attempted to provide a collection of structured and related activities in a specific sequence that produces different outcomes and ensure that the proposed CSTF can be applied to real-world settings. The objective is met via Chapter 6 in which different phases of distinct activities are introduced that guide organization to structure their cloud migration from start to finish based on the artefacts of CSTF as proposed in Chapter 5. The activities consist of important exercises that range from: analyzing stakeholders involved in the project; analyzing the organizational context; identifying and classifying assets that are being migrated to the cloud, performing a risk assessment on the assets; specifying requirements for the assets; and performing audit to determine how requirements are being satisfied by the CSP. All these activities and others are combined together to create a process for implementing the CSTF. Essentially, to ensure adaptability and diverseness, the activities are created in consideration and by following an assortment of industry best practices, guidelines and standards that are generally applicable to all types of organizations regardless of size or industry. Section 7.2 of the Chapter presented a Unified Approach to CSTF process wherein the sections taken from industry standards, best practices and guidelines used in forming the activities are presented. The risk management activity considered STRIDE (Swiderski and Snyder, 2004) and DREAD (Shostack, 2008) models; OWASP (OWASP Cloud - 10 Project, 2014) and ENISA (ENISA, 2009); and CIS CSC(Centre for Internet Security, 2018) and (ENISA, 2016) for developing threats profile, risk register and controls respectively. Also, CSA CCM(Cloud Security Alliance, 2017a) is adopted for the specification of requirements activity. For the audit activity, ISAE 500 Standard (ISAE500), CSA CAIQ (Cloud Security Alliance, 2017b), ISA 200-700 (ISA, 2016), SAS 70(American Institute of Certified Public Accountants. Auditing Standards Board, 1997) are adopted.

9.2.3 Develop a Security Transparency Tool

Objective 3 aimed at developing an assessment tool that enables organizations to collect evidence, probe and assess CSP's conformance to established requirements, and for recommending remedial actions in areas where improvements are needed. The objective is drawn by considering the limitations associated with existing works, approaches and tools that have been designed to foster security transparency such as CSA CAIQ (Cloud Security Alliance, 2017b). For example, CAIQ provides a comprehensive checklist that cloud users can ask for and receive information about CSP services; however, CAIQ does not support users to collect and analyze, and establish findings based on the analysis. Therefore, this Objective is fulfilled via Chapter 6. The Chapter has successfully designed and implemented a proposed tool called STAT (Security Transparency and Audit Tool) that is built to serve as a supporting platform that automates the audit activity within CSTF. The limitations have been addressed by incorporating evidence collection, analysis and reporting routines. By addressing these limitations, STAT enables security auditors delegated by an organisation, to probe the activities of a CSP by seeking information about specific requirements, receiving evidence about how the requirements are being met, establishing assurances about the degree to which the CSP fulfils requirements, and making recommendations for remedial actions. The primary objective of STAT is to facilitate the collection and analysis of evidence, including the establishment of subjective audit judgement and determination of the necessary course of actions that needs to be taken, thereby promoting security transparency in the cloud. Section 8.6 provided a detailed overview of the features that are supported by STAT which are included in three main dashboards: the administrative, cloud auditor and CSP dashboards.

9.3 Research Limitations

While the primary aims and objectives set out for this research have been achieved, the research is not entirely free of lacks. During implementation and evaluation, the researcher has taken note of several shortcomings and limitations facing the research. The major limitations of the research are summarized as:

- **Time constraints:** time constraints was the major factor that limited this research work, which resulted in many intended research activities, particularly for enhancing the proposed framework and tool, not being accomplished. However, the unaccomplished research activities are considered for future research and are described in the section that follows.

- **Empirical Evaluation:** another notable limiting factor for this research is the empirical evaluation method that covered only two case-studies. The evaluation part of CSTF and STAT enabled the researcher to collect and analyze feedback from stakeholders' perception and acceptability of the proposed framework and tool respectively. The limited number of case-studies used and responses collected could potentially impact the

research's generalization. The findings would have been more extensive if more case studies had been covered.

- **Implementation Bottlenecks:** during the implementation phase of CSTF, some bottlenecks unfolded that were not predicted during the development phase of the proposed framework. These included misconception and/or misinterpretation of some of the steps involved. Specifically, most of the activities in the framework, such as risk management, are mostly carried out manually without the application of automated techniques. This resulted in a human error due to some stakeholders misunderstanding the procedures of following the step. The involvement of the researcher curtailed this problem; however, it could be a potential issue when generally adopted.

- **Evidence Assessment:** the current deployment of STAT involves manual assessment of evidence produced by the CSP. Evidence collected are subjectively analyzed and compared to a defined set of criteria for interpretation and establishing conformance to requirements and areas where CSP practices need improvements. A noticeable limitation in this regard is that STAT does not support an automated assessment of evidence, which could be resource and time-consuming.

- **Scalability to broader contexts:** although the target beneficiaries of the proposed framework are companies of all size, especially small and medium-sized, the scalability and adaptability of the framework to accommodate diverse and changing environments like that of large enterprises who have complex systems and immense requirements is not performed. Therefore, there is a need to apply the research to the context of large businesses to establish its suitability to attune diverse contexts.

9.4 Further Research

The previous section had identified some of the crucial limitations observed in this research. This research has unlocked the potentials for different research directions and works in the area of cloud transparency. It is important to outline the direction of future research and how some of the above-mentioned limitations can be addressed.

- I**ntegration of Supplementary Concepts:** extensive research was carried out in the area of cloud security transparency, and numerous concepts were established and used to develop the framework. These concepts enabled the modelling of security transparency by considering various domains such as risk management and audit and they have provided the foundation on which to improve the scope and boundary of transparency in the cloud. Vital future work can focus on identifying and integrating supplementary concepts to accommodate other essential domains of concern such as cost-related transparency and vendor lock-in in the cloud services.

- **Automation of the Overall CSTF Process:** another potential future research is the complete automation of the activities and steps involved in the CSTF process. Full automation of the process will ensure that every activity is performed with consistency and accuracy and reduce the chances of human error. Also, it will provide time-saving by reducing the time and the number of personnel required to undertake each activity. Further, the automation of CSTF process will also improve reliability, thereby leading to wider acceptability amongst businesses.

- **Integration with artificial intelligence:** another future research area is the application of artificial intelligence and machine learning techniques for collecting, processing, and analyzing evidence, as well as for predicting certain anomalies that could result to breachinging of requirements. This will mostly consist of designing or creating a set of rules that enable auditors to direct, optimize and deliver assessment results, which will ensure better assessment and optimization of findings, as well as avoiding bias in audit judgement.

- **Evaluation with Large Scale Companies:** the evaluation of CSTF and STAT was performed in proportionately medium-sized case-studies contexts. Nevertheless, there is a need for further validation in more onerous and larger-scale situations. Therefore, a potential research area is the adjustment and application of the proposed framework to large scale scenarios for testing its efficacy to address enterprise-scale security transparency needs.

9.6 Summary

Lack of security transparency is becoming an increasingly important concern for businesses who entrust their information assets with a CSP. The significance of security transparency is expanding, even more, every day as businesses are growingly concerned about the level of visibility rendered by cloud services, which also adversely affect user trust. There is the dire need tor a viable solution that supports companies to systematically have visibility into cloud activities, methodically track and probe how salient requirements are being fulfilled. This doctoral thesis contributes in that direction by proposing a comprehensive framework and a tool to support the accomplishment of security transparency, which potentially improves businesses trust in cloud services. We believe that the proposed framework, its process and supporting tool will have a significant impact on the cloud computing domain and state-of-the-art in general.

References

A4 Cloud (2017) *Accountability in the Cloud* Available at: http://a4cloud.eu/Accountability.html (Accessed: 20/12/2017 2017).

Aceto, G., Botta, A., de Donato, W. and Pescapè, A. (2013) 'Cloud monitoring: A survey', *Computer Networks,* 57(9), pp. 2093-2115.

Alhamazani, K., Ranjan, R., Mitra, K., Rabhi, F., Jayaraman, P. P., Khan, S. U., Guabtni, A. and Bhatnagar, V. (2015) 'An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art', *Computing,* 97(4), pp. 357-377.

Alzetta, G. (1997) 'INDUCED TRANSPARENCY', *Physics Today,* 50(7), pp. 36.

Amaratunga, D., Baldry, D., Sarshar, M. and Newton, R. (2002) 'Quantitative and qualitative research in the built environment: application of "mixed" research approach', *Work study,* 51(1), pp. 17-31.

American Institute of Certified Public Accountants. Auditing Standards Board (1997) *Consideration of Fraud in a Financial Statement Audit:(supersedes Statement on Auditing Standards No. 53, AICPA, Professional Standards, Vol. 1, AU Sec. 316; and Amends AU Sec. 110," Responsibilities and Functions of the Independent Auditor" and AU Sec. 230," Due Care in the Performance of Work" of Statement on Auditing Standards No. 1, AICPA, Professional Standards, Vol. 1, and Statement on Auditing Standards No. 47, AICPA, Professional Standards, Vol. 1, AU Sec. 312).* American Institute of Certified Public Accountants.

Antoniou, G. and Van Harmelen, F. (2004) 'Web ontology language: Owl', *Handbook on ontologies*: Springer, pp. 67-92.

Argyris, C. and Schön, D. A. (1997) 'Organizational learning: A theory of action perspective', *Reis,* (77/78), pp. 345-348.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A. and Stoica, I. (2009) *Above the clouds: A berkeley view of cloud computing*: Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley.

Arshad, J., Townend, P. and Xu, J. (2013) 'A novel intrusion severity analysis approach for Clouds', *Future Generation Computer Systems,* 29(1), pp. 416-428.

Aslam, M. (2014) *Bringing Visibility in the Clouds: using Security, Transparency and Assurance Services.* Mälardalen University.

Ateniese, G., Burns, R., Curtmola, R., Herring, J., Khan, O., Kissner, L., Peterson, Z. and Song, D. (2011) 'Remote data checking using provable data possession', *ACM Transactions on Information and System Security (TISSEC),* 14(1), pp. 12.

Azarmi, M., Bhargava, B., Angin, P., Ranchal, R., Ahmed, N., Sinclair, A., Linderman, M. and Othmane, L. B. 'An end-to-end security auditing approach for service oriented architectures'. *2012 IEEE 31st Symposium on Reliable Distributed Systems*: IEEE, 279-284.

Azarmi, M., Bhargava, B., Angin, P., Ranchal, R., Ahmed, N., Sinclair, A., Linderman, M. and Othmane, L. B. (2012b) 'An End-to-End Security Auditing Approach for Service Oriented Architectures', pp. 279-284.

Beer, S. (1984) 'The viable system model: Its provenance, development, methodology and pathology', *Journal of the operational research society,* 35(1), pp. 7-25.

Benbasat, I., Goldstein, D. K. and Mead, M. (1987) 'The case research strategy in studies of information systems', *MIS quarterly*, pp. 369-386.

Bhadauria, R., Chaki, R., Chaki, N. and Sanyal, S. (2011) 'A survey on security issues in cloud computing', *IEEE Communications Surveys and Tutorials*, pp. 1-15.

Boudreau, M.-C., Gefen, D. and Straub, D. W. (2001) 'Validation in information systems research: a state-of-the-art assessment', *MIS quarterly*, pp. 1-16.

Brodkin, J. (2008) 'Gartner: Seven cloud-computing security risks', *Infoworld,* 2008, pp. 1-3.

Bryman, A. (2006) 'Integrating quantitative and qualitative research: how is it done?', *Qualitative research,* 6(1), pp. 97-113.

Budgen, D. and Brereton, P. 'Performing systematic literature reviews in software engineering'. *Proceedings of the 28th international conference on Software engineering*: ACM, 1051-1052.

Burns, R. B. and Bursn, R. B. (2000) 'Introduction to research methods'.

Bushman, R. M., Piotroski, J. D. and Smith, A. J. (2004) 'What determines corporate transparency?', *Journal of accounting research,* 42(2), pp. 207-252.

Cappelli, C., Cunha, H., Gonzalez-Baixauli, B. and do Prado Leite, J. C. S. 'Transparency versus security: early analysis of antagonistic requirements'. *Proceedings of the 2010 ACM symposium on applied computing*: ACM, 298-305.

Cassell, C. and Symon, G. (2004) *Essential guide to qualitative methods in organizational research.* Sage.

Castro, J., Kolp, M. and Mylopoulos, J. (2002) 'Towards requirements-driven information systems engineering: the Tropos project', *Information systems,* 27(6), pp. 365-389.

Centre for Internet Security (2018) *The Critical Security Controls for Effective Cyber Defense*. Available at: file://dl-stud1/users/d35/u0852138/Downloads/CIS%20Controls%20Version%207%20(1).pdf (Accessed: 18/05/2018 2018).
Chen, P. P.-S. (1976) 'The entity-relationship model—toward a unified view of data', *ACM Transactions on Database Systems (TODS),* 1(1), pp. 9-36.
Chung, L., Nixon, B. A., Yu, E. and Mylopoulos, J. (2012) *Non-functional requirements in software engineering.* Springer Science & Business Media.
Clocksin, W. F. and Mellish, C. S. (2012) *Programming in Prolog: Using the ISO standard.* Springer Science & Business Media.
Cloud Security Alliance (2017a) *Cloud Controls Matrix v3.0.1 (9-1-17 Update)*. Available at: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/ (Accessed: 02/10/2017 2017).
Cloud Security Alliance (2017b) *Consensus Assessments Initiative Questionnaire* Available at: https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1/ (Accessed: 25/06/2018 2018).
CloudSecurityAlliance (2010) *CloudTrust Protocol*. Available at: https://cloudsecurityalliance.org/group/cloudtrust-protocol/#_overview (Accessed: 20/10/2017 2017).
Conallen, J. (2002) *Building Web applications with UML.* Addison-Wesley Longman Publishing Co., Inc.
Costa, A., Duperoy, T. and Sabella, K. (1991) 'PARTICIPATORY ACTION RESEARCH (PAR)'.
Creswell, J. W. and Creswell, J. D. (2017) *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage publications.
Creswell, J. W., Plano Clark, V. L., Gutmann, M. L. and Hanson, W. E. (2003) 'Advanced mixed methods research designs', *Handbook of mixed methods in social and behavioral research,* 209, pp. 240.
Davis, F. D. (1989) 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', *MIS quarterly*, pp. 319-340.
Denning, D. E. R. (1999) *Information warfare and security.* Addison-Wesley Reading, MA.
Denzin, N. K. and Lincoln, Y. S. (1994) *Handbook of qualitative research.* Sage publications, inc.
Deshpande, S. M. and Ainapure, B. 'An Intelligent Virtual Machine Monitoring System Using KVM for Reliable And Secure Environment in Cloud'. *Advances in Electronics, Communication and Computer Technology (ICAECCT), 2016 IEEE International Conference on*: IEEE, 314-319.
Dillon, T., Wu, C. and Chang, E. 'Cloud computing: issues and challenges'. *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*: Ieee, 27-33.
do Prado Leite, J. C. S. and Cappelli, C. (2010) 'Software transparency', *Business & Information Systems Engineering,* 2(3), pp. 127-139.
Doelitzscher, F. (2014) 'Security audit compliance for cloud computing'.
Drago, I., Mellia, M., M Munafo, M., Sperotto, A., Sadre, R. and Pras, A. 'Inside dropbox: understanding personal cloud storage services'. *Proceedings of the 2012 ACM conference on Internet measurement conference*: ACM, 481-494.
Eisenhardt, K. M. (1989) 'Building theories from case study research', *Academy of management review,* 14(4), pp. 532-550.
ENISA (2016) *Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers* Available at: file://dl-stud1/users/d35/u0852138/Downloads/WP2016%203-2%204%20Technical%20guidelines%20for%20implementation%20of%20minimum%20security%20measures%20(3).pdf (Accessed: 06/05/2018 2016).
ENISA, C. C. (2009) 'Benefits, risks and recommendations for information security', *European Network and Information Security*.
Etzioni, A. (2010) 'Is transparency the best disinfectant?', *Journal of Political Philosophy,* 18(4), pp. 389-404.
EuroCloud Star Audit (2015) *Audit Certification for Cloud Services* Available at: https://staraudit.org/ (Accessed: 19/10/2017 2017).
European Network and Information Security Agency (2009) *Cloud Computing Security Risk Assessment*. Available at: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment (Accessed: 05/08/2017 2017).
European Network and Information Security Agency (2010) *Cloud Computing Information Assurance Framework*. Available at: https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework (Accessed: 09/01/2018 2018).
Fox, J. (2007) 'The uncertain relationship between transparency and accountability', *Development in practice,* 17(4-5), pp. 663-671.
Frentrup, M. and Theuvsen, L. (2006) 'Transparency in supply chains: Is trust a limiting factor', *Trust and Risk in Business Networks, ILB-Press, Bonn*, pp. 65-74.

Garrison, G., Kim, S. and Wakefield, R. L. (2012) 'Success factors for deploying cloud computing', *Communications of the ACM,* 55(9), pp. 62-68.
Giorgini, P., Mouratidis, H. and Zannone, N. (2007) 'Modelling security and trust with secure tropos', *Integrating Security and Software Engineering: Advances and Future Visions*: IGI Global, pp. 160-189.
Glass, M. K., Le Scouarnec, Y., Naramore, E., Mailer, G., Stolz, J. and Gerner, J. (2004) *Beginning PHP, Apache, MySQL Web Development.* John Wiley & Sons.
Goodpaster, K. E. (1991) 'Business ethics and stakeholder analysis', *Business ethics quarterly*, pp. 53-73.
Greene, S. S. (2006) *Security policies and procedures.* New Jersey: Pearson Education.
Grossman, R. L. (2009) 'The case for cloud computing', *IT professional,* 11(2), pp. 23-27.
Hall, M. (2001) *More servlets and JavaServer pages.* Prentice Hall PTR.
Happe, J., Theilmann, W., Edmonds, A. and Kearney, K. T. (2011) 'A reference architecture for multi-level SLA management', *Service Level Agreements for Cloud Computing*: Springer, pp. 13-26.
Hashizume1, K., Rosado, D. G., Fernández-Medina, E. and Fernandez, E. B. (2013) 'An Analysis of Security Issues for Cloud Computing', *Journal of Internet Services and Applications,* 4(5), pp. 1-13.
Heald, D. (2012) 'Why is transparency about public expenditure so elusive?', *International Review of Administrative Sciences,* 78(1), pp. 30-49.
Hickson, I. and Hyatt, D. (2011) 'Html5', *W3C Working Draft WD-html5-20110525, May*.
Höne, K. and Eloff, J. H. P. (2002) 'Information security policy—what do international information security standards say?', *Computers & Security,* 21(5), pp. 402-409.
Ibrahim, A. S., Hamlyn-Harris, J., Grundy, J. and Almorsy, M. 'Cloudsec: a security monitoring appliance for virtual machines in the iaas cloud model'. *Network and System Security (NSS), 2011 5th International Conference on*: IEEE, 113-120.
International Organization for Standardization (1989) *Information Processing Systems: Open Systems Interconnection: LOTOS: a Formal Description Technique Based on the Temporal Ordering of Observational Behaviour.* International Organization for Standardization.
International Standard on Auditing (2016) *Modifications to the Opinion in the Independent Auditor's Report* Available at: https://www.frc.org.uk/getattachment/1ee0a5be-cd77-4439-aa73-7e116c282272/ISA-(UK)-705-Revised-June-2016_final.pdf (Accessed: 22/04/2018 2018).
ISA, I. S. o. A. (2016) *Handbook of International Quality Control, Auditing, Review, Other Assurance and Related Services Pronouncements*. Available at: https://www.kacr.cz/file/4133/2016-2017-iaasb-handbook-volume-1.pdf (Accessed: 11/02/2018 2018).
ISAE500, I. S. o. A. *ISAE 500 A*. Available at: http://www.ifac.org/system/files/downloads/a022-2010-iaasb-handbook-isa-500.pdf (Accessed: 20/03/2018 2018).
Ismail, U. M., Islam, S. and Mouratidis, H. 'Cloud Security Audit for Migration and Continuous Monitoring'. *Trustcom/BigDataSE/ISPA, 2015 IEEE*: IEEE, 1081-1087.
Jia, L., Zhu, M. and Tu, B. 'T-VMI: Trusted Virtual Machine Introspection in Cloud Environments'. *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*: IEEE Press, 478-487.
Johnson, R. E. and Foote, B. (1988) 'Designing reusable classes', *Journal of object-oriented programming,* 1(2), pp. 22-35.
Kalloniatis, C., Mouratidis, H. and Islam, S. (2013) 'Evaluating cloud deployment scenarios based on security and privacy requirements', *Requirements Engineering,* 18(4), pp. 299-319.
Kandukuri, B. R. and Rakshit, A. 'Cloud security issues'. *Services Computing, 2009. SCC'09. IEEE International Conference on*: IEEE, 517-520.
Keele, S. (2007) 'Guidelines for performing systematic literature reviews in software engineering', *Technical report, Ver. 2.3 EBSE Technical Report. EBSE*: sn.
Kemmis, S. and McTaggart, R. (2005) *Participatory action research: Communicative action and the public sphere.* Sage Publications Ltd.
Kitchenham, B. (2004) 'Procedures for performing systematic reviews', *Keele, UK, Keele University,* 33(2004), pp. 1-26.
Knight, S.-a. and Burn, J. (2005) 'Developing a framework for assessing information quality on the World Wide Web', *Informing Science,* 8.
Kosack, S. and Fung, A. (2014) 'Does transparency improve governance?', *Annual Review of Political Science,* 17, pp. 65-87.
Kothari, C. R. (2004) *Research methodology: Methods and techniques.* New Age International.
Krautheim, F. J. (2009) 'Private Virtual Infrastructure for Cloud Computing', *HotCloud,* 9, pp. 2009.1-5.
Krutz, R. L. and Vines, R. D. (2010) *Cloud security: A comprehensive guide to secure cloud computing.* Wiley Publishing.
Kumar, S. and Phrommathed, P. (2005) *Research methodology.* Springer.
L BERG, B. (2001) 'Qualitative research methods for the social sciences'.

Lambrix, P. and Tan, H. 'A framework for aligning ontologies'. *International Workshop on Principles and Practice of Semantic Web Reasoning*: Springer, 17-31.
Lerdorf, R., Tatroe, K. and MacIntyre, P. (2006) *Programming Php.* " O'Reilly Media, Inc.".
Lewis, S. (2015) 'Qualitative inquiry and research design: Choosing among five approaches', *Health promotion practice,* 16(4), pp. 473-475.
Lindstedt, C. and Naurin, D. (2010) 'Transparency is not enough: Making transparency effective in reducing corruption', *International political science review,* 31(3), pp. 301-322.
Mackenzie, N. and Knipe, S. (2006) 'Research dilemmas: Paradigms, methods and methodology', *Issues in educational research,* 16(2), pp. 193-205.
Maedche, A. and Staab, S. (2001) 'Ontology learning for the semantic web', *IEEE Intelligent systems,* 16(2), pp. 72-79.
Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011) 'Cloud computing—The business perspective', *Decision support systems,* 51(1), pp. 176-189.
Maxwell, J. A. (2012) *Qualitative research design: An interactive approach.* Sage publications.
McCarthy, J. (2007) 'The ingredients of financial transparency', *Nonprofit and Voluntary Sector Quarterly,* 36(1), pp. 156-164.
McGuinness, D. L. and Van Harmelen, F. (2004) 'OWL web ontology language overview', *W3C recommendation,* 10(10), pp. 2004.
Mell, P. and Grance, T. (2009) 'The NIST definition of cloud computing', *National institute of standards and technology,* 53(6), pp. 50.
Mills, G. E. (2000) *Action research: A guide for the teacher researcher.* ERIC.
Mouratidis, H. and Giorgini, P. (2007) 'Secure tropos: a security-oriented extension of the tropos methodology', *International Journal of Software Engineering and Knowledge Engineering,* 17(02), pp. 285-309.
Mugenda, A. (2003) 'Research methods Quantitative and qualitative approaches by Mugenda', *Nairobi, Kenya*.
Naurin, D. (2006) 'Transparency, publicity, accountability-The missing links', *Swiss Political Science Review,* 12(3), pp. 90.
Neuman, W. L. (2013) *Social research methods: Qualitative and quantitative approaches.* Pearson education.
Nonde, L., El-Gorashi, T. E. and Elmirghani, J. M. (2015) 'Energy efficient virtual network embedding for cloud networks', *Journal of Lightwave Technology,* 33(9), pp. 1828-1849.
Oates, B. J. (2005) *Researching information systems and computing.* Sage.
Okoli, C. and Schabram, K. (2010) 'A guide to conducting a systematic literature review of information systems research'.
Open Web Application Security Project (2014) *OWASP Risk Rating Methodology*. Available at: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (Accessed: 05/02/2018 2018).
Orlikowski, W. J. and Baroudi, J. J. (1991) 'Studying information technology in organizations: Research approaches and assumptions', *Information systems research,* 2(1), pp. 1-28.
Ouedraogo, M., Dubois, E., Khadraoui, D., Poggi, S. and Chenal, B. 'Adopting an Agent and Event Driven Approach for Enabling Mutual Auditability and Security Transparency in Cloud based Services'. *CLOSER*, 565-572.
Ouedraogo, M., Dubois, E., Khadraoui, D., Poggi, S. and Chenal, B. 'Adopting an agent and event driven approach for enabling mutual auditability and security transparency in cloud based services'. *Proceedings of the International Conference on Cloud Computing and Services Science, Lisbon, Portugal*, 20-22.
Ouedraogo, M. and Mouratidis, H. (2013) 'Selecting a cloud service provider in the age of cybercrime', *Computers & Security,* 38, pp. 3-13.
OWASP Cloud - 10 Project (2014) *Cloud Top 10 Security risks* Available at: https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project 2018).
Pauley, W. (2010) 'CSP transparency: An empirical evaluation', *IEEE Security & Privacy,* 8(6), pp. 32-39.
Pearson, S. and Benameur, A. 'Privacy, security and trust issues arising from cloud computing'. *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*: IEEE, 693-702.
Pearson, S., Tountopoulos, V., Catteddu, D., Südholt, M., Molva, R., Reich, C., Fischer-Hübner, S., Millard, C., Lotz, V. and Jaatun, M. G. 'Accountability for cloud and other future internet services'. *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*: IEEE, 629-632.
Polkinghorne, D. E. (2005) 'Language and meaning: Data collection in qualitative research', *Journal of counseling psychology,* 52(2), pp. 137.

Popović, K. and Hocenski, Ž. 'Cloud computing security issues and challenges'. *MIPRO, 2010 proceedings of the 33rd international convention*: IEEE, 344-349.
Premkumar, G. and Bhattacherjee, A. (2008) 'Explaining information technology usage: A test of competing models', *Omega,* 36(1), pp. 64-75.
Qian, L., Luo, Z., Du, Y. and Guo, L. (2009) 'Cloud computing: An overview', *Cloud computing*, pp. 626-631.
Rak, M., Liccardo, L. and Aversa, R. 'A SLA-based interface for security management in cloud and GRID integrations'. *Information Assurance and Security (IAS), 2011 7th International Conference on*: IEEE, 378-383.
Ramgovind, S., Eloff, M. M. and Smith, E. 'The management of security in cloud computing'. *Information Security for South Africa (ISSA), 2010*: IEEE, 1-7.
Rees, J., Bandyopadhyay, S. and Spafford, E. H. (2003) 'PFIRES: a policy framework for information security', *Communications of the ACM,* 46(7), pp. 101-106.
Rittinghouse, J. W. and Ransome, J. F. (2016) *Cloud computing: implementation, management, and security.* CRC press.
Runeson, P. and Höst, M. (2009) 'Guidelines for conducting and reporting case study research in software engineering', *Empirical software engineering,* 14(2), pp. 131.
Shaikh, F. B. and Haider, S. 'Security threats in cloud computing'. *Internet technology and secured transactions (ICITST), 2011 international conference for*: IEEE, 214-219.
Shostack, A. 'Experiences threat modeling at microsoft'. *Modeling Security Workshop. Dept. of Computing, Lancaster University, UK*.
Sookhak, M., Akhunzada, A., Gani, A., Khurram Khan, M. and Anuar, N. B. (2014) 'Towards dynamic remote data auditing in computational clouds', *ScientificWorldJournal,* 2014, pp. 269357.
Spanoudakis, G. and Mahbub, K. 'Requirements monitoring for service-based systems: Towards a framework based on event calculus'. *Proceedings of the 19th IEEE international conference on Automated software engineering*: IEEE Computer Society, 379-384.
Spring, J. (2011) 'Monitoring cloud computing by layer, part 1', *Security & Privacy, IEEE,* 9(2), pp. 66-68.
Spyns, P., Meersman, R. and Jarrar, M. (2002) 'Data modelling versus ontology engineering', *ACM SIGMod Record,* 31(4), pp. 12-17.
Stevens, R., Goble, C. A. and Bechhofer, S. (2000) 'Ontology-based knowledge representation for bioinformatics', *Briefings in bioinformatics,* 1(4), pp. 398-414.
Straub, D., Boudreau, M.-C. and Gefen, D. (2004) 'Validation guidelines for IS positivist research', *Communications of the Association for Information systems,* 13(1), pp. 24.
Subashini, S. and Kavitha, V. (2011) 'A survey on security issues in service delivery models of cloud computing', *Journal of network and computer applications,* 34(1), pp. 1-11.
Succar, B. (2009) 'Building information modelling framework: A research and delivery foundation for industry stakeholders', *Automation in construction,* 18(3), pp. 357-375.
Swiderski, F. and Snyder, W. (2004) *Threat Modeling (Microsoft Professional).* Microsoft Press.
Theilmann, W., Yahyapour, R. and Butler, J. 'Multi-level sla management for service-oriented infrastructures'. *European Conference on a Service-Based Internet*: Springer, 324-335.
Thong, J. Y. (1999) 'An integrated model of information systems adoption in small businesses', *Journal of management information systems,* 15(4), pp. 187-214.
Top Threats Working Group (2017) 'The Treacherous 12: Cloud Computing Top Threats in 2016', *Cloud Security Alliance. online at https://downloads. cloudsecurityalliance. org/assets/research/topthreats/Treacherous12_CloudComputing_TopThreats. pdf. Accessed,* 1.
Tovarňák, D., Nguyen, F. and Pitner, T. (2014) 'Distributed event-driven model for intelligent monitoring of cloud datacenters', *Intelligent Distributed Computing VII*: Springer, pp. 87-92.
Truong, H.-L. and Dustdar, S. (2010) 'Composable cost estimation and monitoring for computational applications in cloud computing environments', *Procedia Computer Science,* 1(1), pp. 2175-2184.
Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003) 'User acceptance of information technology: Toward a unified view', *MIS quarterly*, pp. 425-478.
Wang, L., Tao, J., Kunze, M., Castellanos, A. C., Kramer, D. and Karl, W. 'Scientific cloud computing: Early definition and experience'. *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on*: Ieee, 825-830.
Whitman, M. E. (2003) 'Enemy at the gate: threats to information security', *Communications of the ACM,* 46(8), pp. 91-95.
Williams, C. A. (1999) 'The securities and exchange commission and corporate social transparency', *Harvard Law Review*, pp. 1197-1311.
Workman, M., Bommer, W. H. and Straub, D. (2008) 'Security lapses and the omission of information security measures: A threat control model and empirical test', *Computers in human behavior,* 24(6), pp. 2799-2816.
Yan, C. (2017) 'CLOUD STORAGE SERVICES'.

Yin, R. K. 'Case study research: Design and methods 4th ed'. *United States: Library of Congress Cataloguing-in-Publication Data*.
Youseff, L., Butrico, M. and Da Silva, D. 'Toward a unified ontology of cloud computing'. *Grid Computing Environments Workshop, 2008. GCE'08*: IEEE, 1-10.
Zachman, J. A. (1987) 'A framework for information systems architecture', *IBM systems journal,* 26(3), pp. 276-292.
Zainal, Z. (2007) 'Case study as a research method', *Jurnal Kemanusiaan,* (9), pp. 1-6.
Zhang, Q., Cheng, L. and Boutaba, R. (2010) 'Cloud computing: state-of-the-art and research challenges', *Journal of internet services and applications,* 1(1), pp. 7-18.
Zissis, D. and Lekkas, D. (2012) 'Addressing cloud computing security issues', *Future Generation computer systems,* 28(3), pp. 583-592.

27001, I. (2013) *ISO 27001: 2013 - Information Technology Security Techniques in Information Security Management Systems Requirements* Available at: https://www.iso.org/standard/54534.html.
A4 Cloud (2017) *Accountability in the Cloud* Available at: http://a4cloud.eu/Accountability.html (Accessed: 20/12/2017 2017).
A Martin, O. A., S New (2018) *Assessing cloud risk: The supply chain perspective*. Available at: https://www.bcs.org/content-hub/assessing-cloud-risk-the-supply-chain-perspective/ (Accessed: 09/10/2019 2019).
Alert Logic, I. (2019) *SIEMless Threat Management* Available at: https://www.alertlogic.com/ 2019).
Almorsy, M., Grundy, J. and Müller, I. (2016) 'An analysis of the cloud computing security problem', *arXiv preprint arXiv:1609.01107*.
Alzetta, G. (1997) 'INDUCED TRANSPARENCY', *Physics Today,* 50(7), pp. 36.
Amaratunga, D., Baldry, D., Sarshar, M. and Newton, R. (2002) 'Quantitative and qualitative research in the built environment: application of "mixed" research approach', *Work study,* 51(1), pp. 17-31.
American Institute of Certified Public Accountants. Auditing Standards Board (1997) *Consideration of Fraud in a Financial Statement Audit:(supersedes Statement on Auditing Standards No. 53, AICPA, Professional Standards, Vol. 1, AU Sec. 316; and Amends AU Sec. 110," Responsibilities and Functions of the Independent Auditor" and AU Sec. 230," Due Care in the Performance of Work" of Statement on Auditing Standards No. 1, AICPA, Professional Standards, Vol. 1, and Statement on Auditing Standards No. 47, AICPA, Professional Standards, Vol. 1, AU Sec. 312).* American Institute of Certified Public Accountants.
Anisetti, M., Ardagna, C. A., Damiani, E., Mana, A. and Spanoudakis, G. (2017) 'Towards transparent and trustworthy cloud', *IEEE Cloud Computing,* 4(3), pp. 40-48.
Antoniou, G. and Van Harmelen, F. (2004) 'Web ontology language: Owl', *Handbook on ontologies*: Springer, pp. 67-92.
Argyris, C. and Schön, D. A. (1997) 'Organizational learning: A theory of action perspective', *Reis,* (77/78), pp. 345-348.
Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A. and Stoica, I. (2009) *Above the clouds: A berkeley view of cloud computing*: Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley.
Aslam, M. (2014) *Bringing Visibility in the Clouds: using Security, Transparency and Assurance Services.* Mälardalen University.
Aujla, G. S., Chaudhary, R., Kumar, N., Das, A. K. and Rodrigues, J. J. (2018) 'SecSVA: secure storage, verification, and auditing of big data in the cloud environment', *IEEE Communications Magazine,* 56(1), pp. 78-85.
Beer, S. (1984) 'The viable system model: Its provenance, development, methodology and pathology', *Journal of the operational research society,* 35(1), pp. 7-25.
Benbasat, I., Goldstein, D. K. and Mead, M. (1987) 'The case research strategy in studies of information systems', *MIS quarterly*, pp. 369-386.
Bhadauria, R., Chaki, R., Chaki, N. and Sanyal, S. (2011) 'A survey on security issues in cloud computing', *IEEE Communications Surveys and Tutorials*, pp. 1-15.
Bhushan, K. and Gupta, B. B. (2017) 'Security challenges in cloud computing: state-of-art', *International Journal of Big Data Intelligence,* 4(2), pp. 81-107.
Borisaniya, B. and Patel, D. (2019) 'Towards virtual machine introspection based security framework for cloud', *Sādhanā,* 44(2), pp. 34.
Boudreau, M.-C., Gefen, D. and Straub, D. W. (2001) 'Validation in information systems research: a state-of-the-art assessment', *MIS quarterly*, pp. 1-16.
Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F. and Mylopoulos, J. (2004) 'Tropos: An agent-oriented software development methodology', *Autonomous Agents and Multi-Agent Systems,* 8(3), pp. 203-236.
Brodkin, J. (2008) 'Gartner: Seven cloud-computing security risks', *Infoworld,* 2008, pp. 1-3.

Bryman, A. (2006) 'Integrating quantitative and qualitative research: how is it done?', *Qualitative research,* 6(1), pp. 97-113.
Burns, R. B. and Bursn, R. B. (2000) 'Introduction to research methods'.
Bushman, R. M., Piotroski, J. D. and Smith, A. J. (2004) 'What determines corporate transparency?', *Journal of accounting research,* 42(2), pp. 207-252.
Cappelli, C., Cunha, H., Gonzalez-Baixauli, B. and do Prado Leite, J. C. S. 'Transparency versus security: early analysis of antagonistic requirements'. *Proceedings of the 2010 ACM symposium on applied computing*: ACM, 298-305.
Casola, V., De Benedictis, A. and Rak, M. 'Security monitoring in the cloud: An sla-based approach'. *Availability, Reliability and Security (ARES), 2015 10th International Conference on*: IEEE, 749-755.
Casola, V., De Benedictis, A., Rak, M. and Villano, U. 'Preliminary Design of a Platform-as-a-Service to Provide Security in Cloud'. *CLOSER*, 752-757.
Cassell, C. and Symon, G. (2004) *Essential guide to qualitative methods in organizational research.* Sage.
Castro, J., Kolp, M. and Mylopoulos, J. (2002) 'Towards requirements-driven information systems engineering: the Tropos project', *Information systems,* 27(6), pp. 365-389.
Centre for Internet Security (2018) *The Critical Security Controls for Effective Cyber Defense*. Available at: file://dl-stud1/users/d35/u0852138/Downloads/CIS%20Controls%20Version%207%20(1).pdf (Accessed: 18/05/2018 2018).
Chang, V., Kuo, Y.-H. and Ramachandran, M. (2016) 'Cloud computing adoption framework: A security framework for business clouds', *Future Generation Computer Systems,* 57, pp. 24-41.
Chen, P. P.-S. (1976) 'The entity-relationship model—toward a unified view of data', *ACM Transactions on Database Systems (TODS),* 1(1), pp. 9-36.
Chung, L., Nixon, B. A., Yu, E. and Mylopoulos, J. (2012) *Non-functional requirements in software engineering.* Springer Science & Business Media.
Cloud Security Alliance (2015) *CSA STAR: The Future of Cloud Trust and Assurance*. Available at: https://cloudsecurityalliance.org/star/#_overview (Accessed: 04-09-2015 2015).
Cloud Security Alliance (2017a) *Cloud Controls Matrix v3.0.1 (9-1-17 Update)*. Available at: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/ (Accessed: 02/10/2017 2017).
Cloud Security Alliance (2017b) *Consensus Assessments Initiative Questionnaire* Available at: https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1/ (Accessed: 25/06/2018 2018).
Cloud Security Alliance (2017c) *Security Trust & Assurance Registry* Available at: https://cloudsecurityalliance.org/star/ (Accessed: 9/02/2017 2019).
CloudSecurityAlliance (2010) *CloudTrust Protocol*. Available at: https://cloudsecurityalliance.org/group/cloudtrust-protocol/#_overview (Accessed: 20/10/2017 2017).
CloudWatch, A. (2019) *Amazon CloudWatch: User Guide*. Available at: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/acw-ug.pdf 2019).
COBIT (2019) *Control Objectives for Information and Related Technology (Cobit)*. Available at: http://www.isaca.org/cobit/pages/default.aspx (Accessed: 03/07/2019 2019).
Conallen, J. (2002) *Building Web applications with UML.* Addison-Wesley Longman Publishing Co., Inc.
Cordón, O. (2011) 'A historical review of evolutionary learning methods for Mamdani-type fuzzy rule-based systems: Designing interpretable genetic fuzzy systems', *International Journal of Approximate Reasoning,* 52(6), pp. 894-913.
Costa, A., Duperoy, T. and Sabella, K. (1991) 'PARTICIPATORY ACTION RESEARCH (PAR)'.
Creswell, J. W. and Creswell, J. D. (2017) *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage publications.
Creswell, J. W., Plano Clark, V. L., Gutmann, M. L. and Hanson, W. E. (2003) 'Advanced mixed methods research designs', *Handbook of mixed methods in social and behavioral research,* 209, pp. 240.
Davis, F. D. (1989) 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', *MIS quarterly*, pp. 319-340.
Denzin, N. K. and Lincoln, Y. S. (1994) *Handbook of qualitative research.* Sage publications, inc.
Deshpande, P., Sharma, S. C., Peddoju, S. K. and Junaid, S. (2018) 'HIDS: A host based intrusion detection system for cloud computing environment', *International Journal of System Assurance Engineering and Management,* 9(3), pp. 567-576.
Deshpande, S. M. and Ainapure, B. 'An Intelligent Virtual Machine Monitoring System Using KVM for Reliable And Secure Environment in Cloud'. *Advances in Electronics, Communication and Computer Technology (ICAECCT), 2016 IEEE International Conference on*: IEEE, 314-319.
do Prado Leite, J. C. S. and Cappelli, C. (2010) 'Software transparency', *Business & Information Systems Engineering,* 2(3), pp. 127-139.

Eisenhardt, K. M. (1989) 'Building theories from case study research', *Academy of management review,* 14(4), pp. 532-550.
ENISA (2016) *Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers* Available at: file://dl-stud1/users/d35/u0852138/Downloads/WP2016%203-2%204%20Technical%20guidelines%20for%20implementation%20of%20minimum%20security%20measures%20(3).pdf (Accessed: 06/05/2018 2016).
ENISA, C. C. (2009) 'Benefits, risks and recommendations for information security', *European Network and Information Security*.
Etzioni, A. (2010) 'Is transparency the best disinfectant?', *Journal of Political Philosophy,* 18(4), pp. 389-404.
European Network and Information Security Agency (2009) *Cloud Computing Security Risk Assessment*. Available at: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment (Accessed: 05/08/2017 2017).
European Network and Information Security Agency (2010) *Cloud Computing Information Assurance Framework*. Available at: https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework (Accessed: 09/01/2018 2018).
Flittner, M., Balaban, S. and Bless, R. 'Cloudinspector: A transparency-as-a-service solution for legal issues in cloud computing'. *2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW)*: IEEE, 94-99.
Fox, J. (2007) 'The uncertain relationship between transparency and accountability', *Development in practice,* 17(4-5), pp. 663-671.
Frentrup, M. and Theuvsen, L. (2006) 'Transparency in supply chains: Is trust a limiting factor', *Trust and Risk in Business Networks, ILB-Press, Bonn*, pp. 65-74.
Garg, S. K., Versteeg, S. and Buyya, R. (2013) 'A framework for ranking of cloud computing services', *Future Generation Computer Systems,* 29(4), pp. 1012-1023.
Garrison, G., Kim, S. and Wakefield, R. L. (2012) 'Success factors for deploying cloud computing', *Communications of the ACM,* 55(9), pp. 62-68.
Giaretta, P. and Guarino, N. (1995) 'Ontologies and knowledge bases towards a terminological clarification', *Towards very large knowledge bases: knowledge building & knowledge sharing,* 25(32), pp. 307-317.
Giorgini, P., Mouratidis, H. and Zannone, N. (2007) 'Modelling security and trust with secure tropos', *Integrating Security and Software Engineering: Advances and Future Visions*: IGI Global, pp. 160-189.
Glass, M. K., Le Scouarnec, Y., Naramore, E., Mailer, G., Stolz, J. and Gerner, J. (2004) *Beginning PHP, Apache, MySQL Web Development.* John Wiley & Sons.
Goodpaster, K. E. (1991) 'Business ethics and stakeholder analysis', *Business ethics quarterly*, pp. 53-73.
Gottschalk, P. (1999) 'Implementation of formal plans: the case of information technology strategy', *Long Range Planning,* 32(3), pp. 362-372.
Gruber, T. (1993) 'What is an Ontology', *WWW Site http://www-ksl. stanford. edu/kst/whatis-an-ontology. html (accessed on 07-09-2004)*.
Hall, M. (2001) *More servlets and JavaServer pages.* Prentice Hall PTR.
Heald, D. (2012) 'Why is transparency about public expenditure so elusive?', *International Review of Administrative Sciences,* 78(1), pp. 30-49.
Hickson, I. and Hyatt, D. (2011) 'Html5', *W3C Working Draft WD-html5-20110525, May*.
Höne, K. and Eloff, J. H. P. (2002) 'Information security policy—what do international information security standards say?', *Computers & Security,* 21(5), pp. 402-409.
IBM (2017) *IBM Security QRadar Version 7.3.2*. Available at: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf 2019).
International Standard on Auditing (2016) *Modifications to the Opinion in the Independent Auditor's Report* Available at: https://www.frc.org.uk/getattachment/1ee0a5be-cd77-4439-aa73-7e116c282272/ISA-(UK)-705-Revised-June-2016_final.pdf (Accessed: 22/04/2018 2018).
ISA, I. S. o. A. (2016) *Handbook of International Quality Control, Auditing, Review, Other Assurance and Related Services Pronouncements*. Available at: https://www.kacr.cz/file/4133/2016-2017-iaasb-handbook-volume-1.pdf (Accessed: 11/02/2018 2018).
ISAE500, I. S. o. A. *ISAE 500 A*. Available at: http://www.ifac.org/system/files/downloads/a022-2010-iaasb-handbook-isa-500.pdf (Accessed: 20/03/2018 2018).
Jaatun, M., Tøndel, I., Moe, N., Cruzes, D., Bernsmed, K. and Haugset, B. (2018) 'Accountability Requirements in the Cloud Provider Chain', *Symmetry,* 10(4), pp. 124.
Jia, L., Zhu, M. and Tu, B. 'T-VMI: Trusted Virtual Machine Introspection in Cloud Environments'. *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*: IEEE Press, 478-487.

Johnson, R. E. and Foote, B. (1988) 'Designing reusable classes', *Journal of object-oriented programming,* 1(2), pp. 22-35.
Jøsang, A. (2016) *Subjective logic.* Springer.
Jouini, M. and Rabai, L. B. A. (2019) 'A security framework for secure cloud computing environments', *Cloud security: Concepts, methodologies, tools, and applications*: IGI Global, pp. 249-263.
Kalloniatis, C., Mouratidis, H. and Islam, S. (2013) 'Evaluating cloud deployment scenarios based on security and privacy requirements', *Requirements Engineering,* 18(4), pp. 299-319.
Kandukuri, B. R. and Rakshit, A. 'Cloud security issues'. *Services Computing, 2009. SCC'09. IEEE International Conference on*: IEEE, 517-520.
Karahanna, E. and Straub, D. W. (1999) 'The psychological origins of perceived usefulness and ease-of-use', *Information & management,* 35(4), pp. 237-250.
Kemmis, S. and McTaggart, R. (2005) *Participatory action research: Communicative action and the public sphere.* Sage Publications Ltd.
Knight, S.-a. and Burn, J. (2005) 'Developing a framework for assessing information quality on the World Wide Web', *Informing Science,* 8.
Kosack, S. and Fung, A. (2014) 'Does transparency improve governance?', *Annual Review of Political Science,* 17, pp. 65-87.
Kothari, C. R. (2004) *Research methodology: Methods and techniques.* New Age International.
Krutz, R. L. and Vines, R. D. (2010) *Cloud security: A comprehensive guide to secure cloud computing.* Wiley Publishing.
Kumar, S. and Phrommathed, P. (2005) *Research methodology.* Springer.
L BERG, B. (2001) 'Qualitative research methods for the social sciences'.
Lambrix, P. and Tan, H. 'A framework for aligning ontologies'. *International Workshop on Principles and Practice of Semantic Web Reasoning*: Springer, 17-31.
Laurén, S. and Leppänen, V. 'Virtual Machine Introspection based Cloud Monitoring Platform'. *Proceedings of the 19th International Conference on Computer Systems and Technologies*: ACM, 104-109.
Leitner, P. and Cito, J. (2016) 'Patterns in the chaos—a study of performance variation and predictability in public iaas clouds', *ACM Transactions on Internet Technology (TOIT),* 16(3), pp. 15.
Lerdorf, R., Tatroe, K. and MacIntyre, P. (2006) *Programming Php.* " O'Reilly Media, Inc.".
Lewis, G. A. 'Role of standards in cloud-computing interoperability'. *2013 46th Hawaii International Conference on System Sciences*: IEEE, 1652-1661.
Lewis, S. (2015) 'Qualitative inquiry and research design: Choosing among five approaches', *Health promotion practice,* 16(4), pp. 473-475.
Li, A., Yang, X., Kandula, S. and Zhang, M. 'CloudCmp: comparing public cloud providers'. *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*: ACM, 1-14.
Lindstedt, C. and Naurin, D. (2010) 'Transparency is not enough: Making transparency effective in reducing corruption', *International political science review,* 31(3), pp. 301-322.
Logentries Inc. (2019) *Logentries*. Available at: https://logentries.com/ 2019).
LogRythm Inc. (2017) *Logrythm*. Available at: https://logrhythm.com/index.html 2019).
MacAfee SIEM (2017) *McAfee Enterprise Security Manager 10.1.0*. Available at: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/27000/PD27123/en_US/esm_1010_pg_en-us.pdf 2019).
Mackenzie, N. and Knipe, S. (2006) 'Research dilemmas: Paradigms, methods and methodology', *Issues in educational research,* 16(2), pp. 193-205.
Maedche, A. and Staab, S. (2001) 'Ontology learning for the semantic web', *IEEE Intelligent systems,* 16(2), pp. 72-79.
Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011) 'Cloud computing—The business perspective', *Decision support systems,* 51(1), pp. 176-189.
Maxwell, J. A. (2012) *Qualitative research design: An interactive approach.* Sage publications.
McCarthy, J. (2007) 'The ingredients of financial transparency', *Nonprofit and Voluntary Sector Quarterly,* 36(1), pp. 156-164.
McGuinness, D. L. and Van Harmelen, F. (2004) 'OWL web ontology language overview', *W3C recommendation,* 10(10), pp. 2004.
Mell, P. and Grance, T. (2009) 'The NIST definition of cloud computing', *National institute of standards and technology,* 53(6), pp. 50.
Menzel, M. and Ranjan, R. 'CloudGenius: decision support for web server cloud migration'. *Proceedings of the 21st international conference on World Wide Web*: ACM, 979-988.
Mills, G. E. (2000) *Action research: A guide for the teacher researcher.* ERIC.
Mouratidis, H. and Giorgini, P. (2007) 'Secure tropos: a security-oriented extension of the tropos methodology', *International Journal of Software Engineering and Knowledge Engineering,* 17(02), pp. 285-309.

Mugenda, A. (2003) 'Research methods Quantitative and qualitative approaches by Mugenda', *Nairobi, Kenya*.
Nagios (2017) *Nagios Core*. Available at: https://www.nagios.org/ 2019).
Naurin, D. (2006) 'Transparency, publicity, accountability-The missing links', *Swiss Political Science Review,* 12(3), pp. 90.
Netsuron EventTracker (2019) *EventTracker*. Available at: https://www.eventtracker.com/ 2019).
Neuman, W. L. (2013) *Social research methods: Qualitative and quantitative approaches.* Pearson education.
Noy, N. F., Sintek, M., Decker, S., Crubézy, M., Fergerson, R. W. and Musen, M. A. (2001) 'Creating semantic web contents with protege-2000', *IEEE intelligent systems,* 16(2), pp. 60-71.
Oates, B. J. (2005) *Researching information systems and computing.* Sage.
Oliveira, T., Thomas, M. and Espadanal, M. (2014) 'Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors', *Information & Management,* 51(5), pp. 497-510.
Open Web Application Security Project (2014) *OWASP Risk Rating Methodology*. Available at: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (Accessed: 05/02/2018 2018).
Orlikowski, W. J. and Baroudi, J. J. (1991) 'Studying information technology in organizations: Research approaches and assumptions', *Information systems research,* 2(1), pp. 1-28.
Ouedraogo, M., Dubois, E., Khadraoui, D., Poggi, S. and Chenal, B. 'Adopting an Agent and Event Driven Approach for Enabling Mutual Auditability and Security Transparency in Cloud based Services'. *CLOSER*, 565-572.
Ouedraogo, M., Dubois, E., Khadraoui, D., Poggi, S. and Chenal, B. 'Adopting an agent and event driven approach for enabling mutual auditability and security transparency in cloud based services'. *Proceedings of the International Conference on Cloud Computing and Services Science, Lisbon, Portugal*, 20-22.
Ouedraogo, M. and Mouratidis, H. (2013) 'Selecting a cloud service provider in the age of cybercrime', *Computers & Security,* 38, pp. 3-13.
OWASP Cloud - 10 Project (2014) *Cloud Top 10 Security risks* Available at: https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project 2018).
Pape, S. R. 2017. Virtual machine introspection facilities. Google Patents.
Pauley, W. (2010) 'Cloud provider transparency: An empirical evaluation', *IEEE Security & Privacy,* 8(6), pp. 32-39.
Pearson, S. and Benameur, A. 'Privacy, security and trust issues arising from cloud computing'. *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*: IEEE, 693-702.
Pearson, S. and Benameur, A. 'Privacy, security and trust issues arising from cloud computing'. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*: IEEE, 693-702.
Pearson, S., Tountopoulos, V., Catteddu, D., Südholt, M., Molva, R., Reich, C., Fischer-Hübner, S., Millard, C., Lotz, V. and Jaatun, M. G. 'Accountability for cloud and other future internet services'. *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*: IEEE, 629-632.
Polkinghorne, D. E. (2005) 'Language and meaning: Data collection in qualitative research', *Journal of counseling psychology,* 52(2), pp. 137.
Premkumar, G. and Bhattacherjee, A. (2008) 'Explaining information technology usage: A test of competing models', *Omega,* 36(1), pp. 64-75.
Proofpoint (2019) *Threat Actors Leverage Credential Dumps, Phishing, and Legacy Email Protocols to Bypass MFA and Breach Cloud Accounts Worldwide*. Available at: https://www.proofpoint.com/us/threat-insight/post/threat-actors-leverage-credential-dumps-phishing-and-legacy-email-protocols 2019).
Qian, L., Luo, Z., Du, Y. and Guo, L. (2009) 'Cloud computing: An overview', *Cloud computing*, pp. 626-631.
Rackspace, I. (2019) *Racskpace Monitoring* Available at: https://developer.rackspace.com/docs/rackspace-monitoring/v1/ 2019).
Ramgovind, S., Eloff, M. M. and Smith, E. 'The management of security in cloud computing'. *Information Security for South Africa (ISSA), 2010*: IEEE, 1-7.
Rao, R. V. and Selvamani, K. (2015) 'Data security challenges and its solutions in cloud computing', *Procedia Computer Science,* 48, pp. 204-209.
Ries, S. 'Certain trust: a trust model for users and agents'. *Proceedings of the 2007 ACM symposium on Applied computing*: ACM, 1599-1604.
Rittinghouse, J. W. and Ransome, J. F. (2016) *Cloud computing: implementation, management, and security.* CRC press.

Rittinghouse, J. W. and Ransome, J. F. (2017) *Cloud computing: implementation, management, and security.* CRC press.
Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S. and Hopkins, P. P. (2010) 'The cloud: understanding the security, privacy and trust challenges', *Privacy and Trust Challenges (November 30, 2010)*.
Runeson, P. and Höst, M. (2009) 'Guidelines for conducting and reporting case study research in software engineering', *Empirical software engineering,* 14(2), pp. 131.
Russell, S. J. and Norvig, P. (2016) *Artificial intelligence: a modern approach.* Malaysia; Pearson Education Limited.
Ryoo, J., Rizvi, S., Aiken, W. and Kissell, J. (2014) 'Cloud security auditing: challenges and emerging approaches', *IEEE Security & Privacy,* 12(6), pp. 68-74.
Saint-Germain, R. (2005) 'Information security management best practice based on ISO/IEC 17799', *INFORMATION MANAGEMENT JOURNAL-PRAIRIE VILLAGE-,* 39(4), pp. 60.
Salesforce, I. (2019) *REST API Developer Guide* Available at: https://developer.salesforce.com/docs/atlas.en-us.api_rest.meta/api_rest/intro_what_is_rest_api.htm 2019).
Shen, L. (2014) 'The NIST cybersecurity framework: Overview and potential impacts', *Scitech Lawyer,* 10(4), pp. 16.
Shen, W., Qin, J., Yu, J., Hao, R. and Hu, J. (2018) 'Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage', *IEEE Transactions on Information Forensics and Security,* 14(2), pp. 331-346.
Shostack, A. 'Experiences threat modeling at microsoft'. *Modeling Security Workshop. Dept. of Computing, Lancaster University, UK*.
Singh, A. and Chatterjee, K. (2017) 'Cloud security issues and challenges: A survey', *Journal of Network and Computer Applications,* 79, pp. 88-115.
Smullyan, R. R. (2012) *First-order logic.* Springer Science & Business Media.
Solutions Review (2017) *Security Information and Event Management - Buyer's Guide* Available at: https://solutionsreview.com/dl/2017_Solutions_Review_SIEM_Buyers_Guide_KKM06.pdf 2019).
Sookhak, M., Akhunzada, A., Gani, A., Khurram Khan, M. and Anuar, N. B. (2014) 'Towards dynamic remote data auditing in computational clouds', *ScientificWorldJournal,* 2014, pp. 269357.
Spyns, P., Meersman, R. and Jarrar, M. (2002) 'Data modelling versus ontology engineering', *ACM SIGMod Record,* 31(4), pp. 12-17.
Stevens, R., Goble, C. A. and Bechhofer, S. (2000) 'Ontology-based knowledge representation for bioinformatics', *Briefings in bioinformatics,* 1(4), pp. 398-414.
Straub, D., Boudreau, M.-C. and Gefen, D. (2004) 'Validation guidelines for IS positivist research', *Communications of the Association for Information systems,* 13(1), pp. 24.
Subashini, S. and Kavitha, V. (2011) 'A survey on security issues in service delivery models of cloud computing', *Journal of network and computer applications,* 34(1), pp. 1-11.
Succar, B. (2009) 'Building information modelling framework: A research and delivery foundation for industry stakeholders', *Automation in construction,* 18(3), pp. 357-375.
Sugeno, M. (1993) 'Fuzzy measures and fuzzy integrals—a survey', *Readings in Fuzzy Sets for Intelligent Systems*: Elsevier, pp. 251-257.
Sumetanupap, A. and Senivongse, T. 'Enhancing service selection with a provider trustworthiness model'. *2011 Eighth International Joint Conference on Computer Science and Software Engineering (JCSSE)*: IEEE, 281-286.
Sun, P. J. (2019) 'Research on the Tradeoff Between Privacy and Trust in Cloud Computing', *IEEE Access,* 7, pp. 10428-10441.
Suneja, S., Koller, R., Isci, C., de Lara, E., Hashemi, A., Bhattacharyya, A. and Amza, C. (2017) 'Safe inspection of live virtual machines', *ACM SIGPLAN Notices,* 52(7), pp. 97-111.
Swiderski, F. and Snyder, W. (2004) *Threat Modeling (Microsoft Professional).* Microsoft Press.
Thong, J. Y. (1999) 'An integrated model of information systems adoption in small businesses', *Journal of management information systems,* 15(4), pp. 187-214.
Tian, H., Chen, Z., Chang, C.-C., Huang, Y., Wang, T., Huang, Z.-a., Cai, Y. and Chen, Y. (2019) 'Public audit for operation behavior logs with error locating in cloud storage', *Soft Computing,* 23(11), pp. 3779-3792.
Top Threats Working Group (2017) 'The Treacherous 12: Cloud Computing Top Threats in 2016', *Cloud Security Alliance. online at https://downloads. cloudsecurityalliance. org/assets/research/topthreats/Treacherous12_CloudComputing_TopThreats. pdf. Accessed,* 1.
Tovarňák, D., Nguyen, F. and Pitner, T. (2014) 'Distributed event-driven model for intelligent monitoring of cloud datacenters', *Intelligent Distributed Computing VII*: Springer, pp. 87-92.

Vaidya, O. S. and Kumar, S. (2006) 'Analytic hierarchy process: An overview of applications', *European Journal of operational research,* 169(1), pp. 1-29.
Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003) 'User acceptance of information technology: Toward a unified view', *MIS quarterly*, pp. 425-478.
Von Solms, B. (2005) 'Information Security governance: COBIT or ISO 17799 or both?', *Computers & Security,* 24(2), pp. 99-104.
Williams, C. A. (1999) 'The securities and exchange commission and corporate social transparency', *Harvard Law Review*, pp. 1197-1311.
Workman, M., Bommer, W. H. and Straub, D. (2008) 'Security lapses and the omission of information security measures: A threat control model and empirical test', *Computers in human behavior,* 24(6), pp. 2799-2816.
Yin, R. K. 'Case study research: Design and methods 4th ed'. *United States: Library of Congress Cataloguing-in-Publication Data*.
Youseff, L., Butrico, M. and Da Silva, D. 'Toward a unified ontology of cloud computing'. *2008 Grid Computing Environments Workshop*: IEEE, 1-10.
Yu, E. S. 'Towards modelling and reasoning support for early-phase requirements engineering'. *Requirements Engineering, 1997., Proceedings of the Third IEEE International Symposium on*: IEEE, 226-235.
Zachman, J. A. (1987) 'A framework for information systems architecture', *IBM systems journal,* 26(3), pp. 276-292.
Zainal, Z. (2007) 'Case study as a research method', *Jurnal Kemanusiaan,* (9), pp. 1-6.
Zhang, Q., Cheng, L. and Boutaba, R. (2010) 'Cloud computing: state-of-the-art and research challenges', *Journal of internet services and applications,* 1(1), pp. 7-18.
Zimmermann, H.-J. (2011) *Fuzzy set theory—and its applications.* Springer Science & Business Media.
Zissis, D. and Lekkas, D. (2012) 'Addressing cloud computing security issues', *Future Generation computer systems,* 28(3), pp. 583-592.

Appendices

Appendix A: Questionnaire Evaluation for Framework Evaluation

Acceptability Ratings for the Proposed Framework

The purpose of this questionnaire is to collect your feedback about the proposed "**A Framework for Security Transparency in Cloud Computing**", which is aimed at supporting your organisation in achieving and enhancing security transparency. Your feedback is highly important in helping us establish the validity of the proposed framework and areas of improvement. Kindly respond to the questions that follow by "checking" one of the boxes where appropriate. The questions are designed and evaluated according to criterion as:

1. Ease of use: enquires whether the framework is designed in such a way that can be easily used by users.
2. Relevance: determines whether the framework is relevant in terms of feasibility for supporting your organisation achieve security transparency
3. Usefulness: whether the framework will be very useful in helping the organisation achieve security transparency.
4. Flexibility and dynamics: whether the framework is dynamic enough to cover and deal with larger contexts and scenarios.
5. Compliance to security standards and best practices: attempts to establish whether the framework complies with industry standards such as ISO27001/2, and NIST
6. Trustworthiness: enquires whether the framework is trustworthy in ensuring the privacy and security, as well as preventing future security issues.

Thank you for your cooperation.

S/N	**Evaluation Criteria**	**Question**	**Response Options**			
			Strongly Agree	**Agree**	**Not Sure**	**Disagree**
1.	Ease of Use	Do you agree that CSTF is clear and easily understandable to intended users?				
2.	Relevance	Do you agree the proposed framework is relevant for supporting organisations achieve security transparency?				
3.	Usefulness	Do you agree that the proposed framework is useful in terms of the expected deliverables**?**				
4.	Flexibility	Do you agree the proposed framework is flexible to adapt to dynamic contexts?				
5.	Compliance with security standards and best practices	Does the framework comply with relevant laws, standards and best practices?				
6.	Trustworthiness	Do you consider the proposed framework to be trustworthy in ensuring privacy and security?				

Appendix B: Questionnaire for Evaluating Security Transparency and Audit Tool Evaluation (STAT)

Acceptability Ratings for the Proposed Security Transparency and Audit Tool (STAT)

The purpose of this questionnaire is to collect your feedback about the proposed "Security Transparency and Audit Tool", which is part of the research titled: "A Framework for Security Transparency in Cloud Computing". The tool is aimed at supporting your organisation in achieving and enhancing security transparency. Your feedback is highly important in helping us establish the validity of the proposed Tool and areas of improvement. Kindly respond to the questions that follow by "checking" one of the boxes where appropriate. The questions are designed and evaluated according to criterion as:

7. Ease of use: enquires whether STAT is considered to be designed in such a way that can be easily used by users.
8. Relevance: determines whether STAT is relevantly feasible to support your organisation in achieving security transparency
9. Usefulness: whether STAT will be very useful in helping the organisation achieve security transparency.
10. Flexibility and dynamics: whether STAT is dynamic enough to cover and deal with larger contexts and scenarios.
11. Compliance to security standards and best practices: attempts to establish whether STAT complies with industry standards such as ISO27001/2, and NIST
12. Trustworthiness: enquires whether STAST is trustworthy in ensuring the privacy and security, as well as preventing future security issues.

Thank you for your cooperation.

S/N	Evaluation Criteria	Question	Response Options			
			Strongly Agree	Agree	Not Sure	Disagree
1.	Ease of Use	Do you agree that CSTF is clear and easily understandable to intended users?				
2.	Relevance	Do you agree the proposed framework is relevant for supporting organisations achieve security transparency?				
	Usefulness	Do you agree that the proposed framework is useful in terms of the expected deliverables**?**				
3.						
	Flexibility	Do you agree the proposed framework is flexible to adapt to dynamic contexts?				
4.						
5.	Compliance with security standards and best practices	Does the framework comply with relevant laws, standards and best practices?				
6.						
7.	Trustworthiness	Do you consider the proposed framework to be trustworthy in ensuring privacy and security?				

Appendix C: Security Audit Checklist

Transparency Requirements

Requirement	Target Verification (Control Domain)	Base Measure (Control Type)	Specification	Question	CSP Response			Means of Verification	Audit Criteria					Conformance Level
					Yes	No	N/A		S	C	U	A	R	
Transparency	Supply chain mgmt., transparency & accountability	Data quality & Integrity	CSP should work with their supply –chain partners to ensure data quality errors and associated risks are prevented. Providers should also design and implement controls to mitigate and contain data security risks through adequate access controls, separation of duties and least privilege access to all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?				Authentication and authorisation logs, third party security audit report, security policies.						
				Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?										
		Incident reporting	Information about security incidents that affected customers should be made available by the CSP through electronic methods such as portals.	Do you make security incident information available to all affected customers through electronic methods?				Events notification mechanisms or platforms, intrusion detection reports, vulnerability scan report, and penetration test reports.						
				Do you provide tenants with capacity planning and usage reports?										
				Do you permit tenants to perform independent vulnerability assessments?										
				Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?										
				Do you log and alert any changes made to virtual machine images regardless of				Virtual resource access and activity reports,						

				their running state (e.g., dormant, off or running)?				security incident management policies and report mechanisms							
				Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)											
				Will you share statistical information for security incident data with your tenants upon request?											
				Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?											
		Provider Internal Assessments	Internal security assessments should be performed at least annually to establish conformance and effectiveness of policies, procedures and supporting measures.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?				Proof of certification and accreditation issued by standards, best practice and independent third-party attestations, industry best practice, and relevant certifications.							
				Do you provide customers with a copy of governing standards, policies and guidelines upon request?											
				Do you notify customers with changes to governing policies, standards and guidelines?											
				Do you have a security policy that is clearly documented and represented to all concerned clients?											
				Do you have a security policy that is augmented by security standards or guidelines?											

				Do you provide customers visibility into independent third party audits?											
				Do you provide customers visibility into assets management?											
		Third party agreement	Supply chain agreements between the CSP and the organisation shall incorporate the scope of business relationship covered and the services offered; information security requirements; notification and/or pre-authorization of any changes controlled by the provider with customer impacts; timely notification of a security incident to customers; assessment and independent verification of compliance with agreement terms; expiration of the business relationship and treatment of customer.	Do you monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?				Contracts management and monitoring certified by independent third-party auditor, compliance to relevant industry certifications, best practice, and relevant certifications,						
				Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?											
				Do you provide clients with a list and copies of all sub processing agreements and keep this updated?											
		Third party providers	There should be reasonable information security across their supply chain, which includes all third-party providers upon which the CSP's information supply chain depends.	Do you have any services that are provided by a third-party?				Contracts management and monitoring certified by independent third-party auditor, compliance to relevant industry certifications, best practice, and relevant certifications.						
				If any part of your services are outsourced, does the providing party comply with the same policy and standards you enforce?											
				Do you audit third party providers for compliance with policies and standards?											
		Audit tools access	There should be appropriate restriction and segmentation	Do you restrict, log, and monitor access to your											

	Identity and access management		access to, and use of audit tools that interact with the organisation's information systems in order to prevent compromise and misuse of log data?	information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?				Authentication and authorisation mechanisms, network activity monitoring, independent third-party attestations to relevant industry certifications, industry best practice, and relevant certifications.						
				Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?											
				Do you monitor and log privileged access (e.g., administrator level) to information security management systems?											
		User access restriction/authorisation	Policies and procedures should be established to ensure identities are only accessible based on rules of least privilege.	Do you document how you grant and approve access to tenant data?											
				Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?											
	Infrastructure & virtualisation Security	Audit detection	A high level of assurance should be provided regarding the protection, retention and policy management of audit logs that adhere to applicable legal, statutory, and regulatory compliance obligations. User access accountability should also be provided for detecting potential suspicious behaviours and/or file integrity anomalies, and supporting forensic investigations in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?				Systems and network intrusion detection and activity monitoring.						
		Independent audits	Intendent reviews and assessments should be	Do you allow tenants to view your SOC2/ISO 27001 or				Proof of compliance with						

	Audit assurance & compliance		performed to support the organisation address nonconformities of established requirements, standards, policies, procedures and compliance obligations.	similar third-party audit or certification reports?				ISO 27001 and other relevant industry standards.						
				Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?											
				Do you conduct internal audits regularly as prescribed by industry best practices and guidance?				Independent third-party attestations to relevant industry certifications, industry best practice, and relevant certifications.							
				Are the results of the penetration tests available to tenants at their request?											
				Are all requirements and trust levels for customers' access defined and documented?											
				Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incident?				Penetration test results, systems and network activity reports, data and systems change report.							
				Is physical and logical user access to audit logs restricted to authorized personnel?											
				Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?											
				Are audit logs centrally stored and retained?											
				Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?											

				Are all requirements and trust levels for customers' access defined and documented?										

Baselined Requirements

Requirement	Target Verification (Control Domain)	Base Measure (Control Type)	Specification	Question	CSP Response			Means of Verification	Audit Criteria					Compliance Level
					Yes	No	N/A		S	C	U	A	R	
Baseline requirements	Datacentre security	Controlled access points	There must be a classification of assets according to business criticality, service-level expectations, and operational continuity requirements of the organisation. A complete inventory of business-critical assets located geographical locations must be maintained and regularly updated, with defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?				Independent third-party attestations to relevant industry certifications, industry best practice, and relevant certifications.						
				Do you maintain a complete inventory of all of your critical supplier relationships?										
		Equipment identification	Prior to granting access request, automated mechanisms should be used to identify connection request based on equipment location.	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?				Independent third-party attestations to relevant industry certifications, industry best practice, and relevant certifications.						
				Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, and replication)?										
		User access	Physical access to facilities storing critical assets must be restricted and controlled.	Do you restrict physical access to information assets and functions by users and support personnel?				Independent third-party attestations to						

				Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?				relevant industry certifications, industry best practice, and relevant certifications						
	Encryption & key mgmt.	Key generation	Policies and procedures for managing cryptographic keys in the cloud service cryptosystem must be established.	Do you have a capability to allow creation of unique encryption keys per tenant?				Independent third-party attestations to relevant industry certifications, industry best practice, and relevant certifications						
				Do you have a capability to manage encryption keys on behalf of tenants?											
				Do you protect encryption keys, and what controls are put in place to effect that?											
		Storage and access	Appropriate platform and data encryption in validated formats and standard algorithms should be implemented, while making sure that keys are not stored in the cloud but maintained by trusted key management provider.	Do you have platform and data appropriate encryption that use open/validated formats and standard algorithms?				Independent third-party attestations to relevant industry certifications, industry best practice, and relevant certifications						
				Do you have procedures in place to manage and recover compromised encryption keys?											
				Do you have a security policy that clearly defines what must be encrypted?											
	Identity & access management	Diagnostic configuration ports access	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?											
		User ID Credentials	User accounts credentials should be restricted in line with appropriate identity entitlement, and access management and	Do you manage accounts with administrator or higher privileges?				Independent third-party attestations to relevant industry						
				Do you verify user identity and registration?											

			according to established policies and procedures	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?				certifications, industry best practice, and relevant certifications. Authentication and authorisation monitoring reports and policies.							
				Do you use open standards to delegate authentication capabilities to your tenants?											
				Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?											
				Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?											
				Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?											
				Do you allow tenants to use third-party identity assurance services?											
				Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?											
				Do you allow tenants/customers to define password and account lockout policies for their accounts?											
				Do you support the ability to force password changes upon first logon?											
				Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service											

				via email, defined challenge questions, manual unlock)?										
		Source code access restriction	Access to applications, programs, object source, and other forms of intellectual property belonging to the organisation should be restricted by following the rules of least privilege based on job function as per established user access policies and procedures of the organisation.	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?				Authentication and authorisation monitoring report						
				Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?				Independent third-party attestations to relevant industry certifications, industry best practice, and relevant certifications, and legal frameworks						
		Utility program access	All utility programs that could potentially override system, object, network, virtual machines and applications should be restricted	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?				Independent third-party attestations to relevant industry certifications, industry best practice, and relevant certifications						
				Do you have the capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?										
				Are attacks that target the virtual infrastructure prevented with technical controls?										
	Human resources	Asset returns	Policies and procedures should be established that ensure organizationally-owned assets are returned within an established period upon the termination or expiration of cloud service contract.	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?				Independent third-party attestations to relevant industry certifications, industry best						
				Is your Privacy Policy aligned with industry standards?										

								practice, and relevant certifications, and legal requirements							

Business Requirements

Requirement	Target Verification (Control Domain)	Base Measure (Control Type)	Specification	Question	CSP Response			Means of Verification	Audit Criteria					Compliance Level
					Yes	No	N/A		S	C	U	A	R	
Business	Business community mgmt. & operational resilience	Business continuity planning	Procedures and policies shall be established for a unified framework that documents and ensures business continuity plans ensures business continuity plan are consistent in addressing priorities for testing, maintenance and development according to organisation's requirements.	Do you provide tenants with geographically resilient hosting options?				Independent third-party attestations to relevant industry certifications, industry best practice, and relevant certifications, and legal requirements.						
				Do you provide tenants with infrastructure service failover capability to other providers?										
		Business continuity testing	There should be planned testing of Implemented business continuity and security incident response plans on regular intervals or upon significant changes to CSP's environmental factors.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?				Independent third-party attestations to relevant industry certifications, industry best practice, and relevant certifications, and legal requirements						
				Does your cloud solution include independent hardware restore and recovery capabilities?										
				If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?										

				If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new CSP?											
				If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?											
				Does your cloud solution include software/provider independent restore and recovery capabilities?											
				Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?											
				Do you have a formal process for contingency plan that guides the process for business continuity?											
				Do you have service recovery point objective (RPO) and recovery time objective (RTO)?											
				Do you have a secondary site for disaster recovery											
		Resource provisioning	Cloud resources should be sufficiently provisioned according to organisation's requirements.	Do you have controls and procedures in place to manage resource exhaustion, including processing oversubscription, storage outage, and network exhaustion?				Cloud resource utilisation and management services							

				Do you limit subscriptions to the service in order to protect SLA agreements?										
				Do you provide customers with utilisation and capacity planning information?										
	Identity & Access Management	Third Party Access	A risk management assessment should be used to identify, assess and prioritise risks posed by business processes requiring third-party access to the organisation's assets. Followed by a coordinated application of resources to minimize, monitor and measure the likelihood and impact of unauthorised access to assets.	Do you provide multi-failure disaster recovery capability?				Independent third-party attestations to relevant industry certifications, industry best practice, and relevant certifications, and legal frameworks.						
				Do you monitor service continuity with upstream providers in the event of provider failure?										
				Do you have more than one provider for each service you depend on?										
				Do you provide access to operational redundancy and continuity summaries, including the services you depend on?										
				Do you provide a tenant-triggered failover option?										
				Do you share your business continuity and redundancy plans with your tenants?										
	Security incident management, e-discovery, & cloud forensics	Incident Response Legal Preparation	Appropriate forensic procedures and processes, including chain of custody should be maintained for the presentation of evidence with the aim of supporting potential legal action subject to relevant jurisdiction after a security incident. An organisation and other external parties impacted should be given the opportunity to participate as per	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?				Independent third-party attestations to relevant industry certifications, industry best practice, relevant certifications, legal and regulatory compliance.						
				Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?										

			legal requirements of forensic investigation.	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?											
				Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?											
				Do you monitor and quantify the types, volumes, and impacts on all information security incidents?											
	Governance and Risk Management	Baseline Requirement	Baseline security requirements that comply with applicable legal, statutory, and regulatory compliance should be established for organizationally-owned assets. Any deviation following change management policies and procedures must be authorise. Compliance with security baseline requirements should be periodically reassessed	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?											
				Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?											
				Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?											

Operational Requirements

Requirement	Target Verification (Control Domain)	Base Measure (Control Type)	Specification	Question	CSP Response			Means of Verification	Audit Criteria					Compliance Level
					Yes	No	N/A		S	C	U	A	R	

Operational	Threat and vulnerability management	Antiviruses/malicious software	Technical measures, including policies and procedures should be established to prevent the execution of malware on organizationally-owned assets	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?				Malware activity monitoring, intrusion detection and prevention reports, Independent third-party attestations to relevant industry certifications, industry best practice, relevant certifications, legal and regulatory compliance.							
				Do you ensure that security threat detection systems using signatures, lists, or behavioural patterns are updated across all infrastructure components within industry accepted time frames?											
		Vulnerability/patch management	Technical measures, policies and procedures should be implemented and established to enable timely detection of vulnerabilities within organizationally-owned assets to ensure the efficiency of security controls. A remediation approach for mitigating vulnerabilities should also be used. The CSP should inform the organisation of policies and procedures and identified weaknesses especially if the organisation is affected by emerging vulnerabilities.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?				Malware activity monitoring report, system and network monitoring reports, Independent third-party audit and attestations to relevant industry certifications, industry best practice, relevant							
				Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?											
				Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?											
				Will you make the results of vulnerability scans available to tenants at their request											
				Do you have a capability to rapidly patch vulnerabilities											

				across all of your computing devices, applications, and systems?				certifications, legal and regulatory compliance.							
	Governance and risk management	Risk assessments	Risk assessments associated with data governance requirements shall be conducted at planned intervals and consider: the awareness of where sensitive data is stored and transmitted. Compliance with defined retention periods and end-of-life disposal requirements; data classification and protection from unauthorised use and access.	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?				Independent third-party audit and attestations to relevant industry certifications, industry best practice, and relevant certifications, legal and regulatory compliance							
				Do you conduct risk assessments associated with data governance requirements at least once a year?											
	Datacentre security	Data centre security and asset management	Processes, procedures and controls should be implemented for ensuring physical security parameters for safeguarding sensitive assets. .	Do you have requirements for controlling physical access to your facility?				Independent third-party audit and attestations to relevant industry certifications, industry best practice, and relevant certifications, legal and regulatory compliance							
				Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) in place?											
				Do you have procedures for risk assessments for physical security											
				Do you maintain and complete inventory of all software, network, hardware and virtual components?											
				Do you support asset categorisation of different sensitivity levels?											
				Do you maintain virtual segregation and physical											

				separation of assets at different sensitivity levels?											
	Application & Interface Security	Application Security	The provisions and recommendations of industry standards should be followed in the design, development, deployment and testing of applications and programming interfaces (APIs) .	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?				Independent third-party audit and attestations to relevant industry certifications, industry best practice, and relevant certifications, legal and regulatory compliance							
				Do you use an automated source code analysis tool to detect security defects in code prior to production?											
				Do you use manual source-code analysis to detect security defects in code prior to production?											
				Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?											
	Interoperability & Portability	APIs	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?				Independent third-party audit and attestations to relevant industry certifications, industry best practice, and relevant certifications, legal and regulatory compliance							
		Data request	All structured and unstructured data shall be available to the customer and provided to them upon request	Is unstructured customer data available on request in an				Independent third-party attestations to							

			in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	industry-standard format (e.g., .doc, .xls, or .pdf)?				relevant industry certifications, industry best practice, and relevant certifications, legal and regulatory compliance						
		Policy & Legal	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?				Independent third-party audit and attestations to relevant industry certifications, industry best practice, and relevant certifications, legal and regulatory compliance						
				Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?										
		Standardized Network Protocols	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?				Independent third-party audit and attestations to relevant industry certifications, industry best practice, and relevant certifications, legal and regulatory compliance						
				Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?										
		Virtualisation	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g.,				Independent third-party audit and attestations to relevant						

			interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	OVF) to help ensure interoperability?				industry certifications, industry best practice, and relevant certifications, legal and regulatory compliance						
				Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review											
	Data Security & Information Lifecycle Management	Classification	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?				Independent third-party audit and attestations to relevant industry certifications, industry best practice, and relevant certifications, legal and regulatory compliance						
				Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?											
				Do you have a capability to use system geographic location as an authentication factor?											
				Can you provide the physical location/geography of storage of a tenant's data upon request?											
				Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation											

Audit Findings/Judgement

Transparency Requirements

Requirement	Target Verification (Control Domain)	Base Measure (Control Type)	Question	Audit Judgement			Remedial Actions		
				Defective	Acceptable	Effective	Preventive	Detective	Corrective
Transparency	Supply chain mgmt., transparency & accountability	Data quality & Integrity	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?		*			*	
			Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?			*			
		Incident reporting	Do you make security incident information available to all affected customers through electronic methods?		*			*	
			Do you provide tenants with capacity planning and usage reports?			*			
			Do you permit tenants to perform independent vulnerability assessments?			*		*	
			Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?			*			
			Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	*			*	*	*
			Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)		*			*	
			Will you share statistical information for security incident data with your tenants upon request?			*			
			Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?			*			*

		Provider Internal Assessments	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?			*			
			Do you provide customers with a copy of governing standards, policies and guidelines upon request?			*			
			Do you notify customers with changes to governing policies, standards and guidelines?			*			
			Do you have a security policy that is clearly documented and represented to all concerned clients?			*			
			Do you have a security policy that is augmented by security standards or guidelines?			*			
			Do you provide customers visibility into independent third party audits?			*			
			Do you provide customers visibility into assets management?			*			
		Third party agreement	Do you monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	*					*
			Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?		*			*	*
			Do you provide clients with a list and copies of all sub-processing agreements and keep this updated?	*					*
		Third-party providers	Do you have any services that are provided by a third-party?		*				*
			If any part of your services are outsourced, does the providing party comply with the same policy and standards you enforce?		*		*		*
			Do you audit third party providers for compliance with policies and standards?		*		*		*
	Identity and access management	Audit tools access	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?			*			
			Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?			*			
			Do you monitor and log privileged access (e.g., administrator level) to information security management systems?						

		User access restriction/authorisation	Do you document how you grant and approve access to tenant data?			*			
			Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	*			*	*	
	Infrastructure & virtualisation Security	Audit detection	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, an investigation by root cause analysis, and response to incidents?			*			
	Audit assurance & compliance	Independent audits	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?			*			
			Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?			*			
			Do you conduct internal audits regularly as prescribed by industry best practices and guidance?			*			
			Are the results of the penetration tests available to tenants at their request?			*			
			Are all requirements and trust levels for customers' access defined and documented?	*					*
			Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, an investigation by root cause analysis, and response to the incident?			*			
			Is physical and logical user access to audit logs restricted to authorized personnel?			*			
			Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?			*			
			Are audit logs centrally stored and retained?			*			
			Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?			*			
			Are all requirements and trust levels for customers' access defined and documented?	*			*	*	

Business Requirements

Requirement	Target Verification (Control Domain)	Base Measure (Control Type)	Question	Audit Findings			Audit Findings Remedial Actions		
				Defective	Acceptable	Effective	Preventive	Detective	Corrective
Business	Business community mgmt. & operational resilience	Business continuity planning	Do you provide tenants with geographically resilient hosting options?			*			
			Do you provide tenants with infrastructure service failover capability to other providers?						
		Business continuity testing	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	*			*		*
			Does your cloud solution include independent hardware restore and recovery capabilities?			*			
			If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?			*			
			If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new CSP?		*				
			If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	*					*
			Does your cloud solution include software/provider-independent restore and recovery capabilities?			*			
			Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?			*			
			Do you have a formal process for a contingency plan that guides the process for business continuity?		*		*		
			Do you have a service recovery point objective (RPO) and recovery time objective (RTO)?			*			
			Do you have a secondary site for disaster recovery			*			
		Resource provisioning	Do you have controls and procedures in place to manage resource exhaustion, including processing			*			

			oversubscription, storage outage, and network exhaustion?						
			Do you limit subscriptions to the service in order to protect SLA agreements?			*			
			Do you provide customers with utilisation and capacity planning information?		*				
	Identity & Access Management	Third-Party Access	Do you provide multi-failure disaster recovery capability?			*			
			Do you monitor service continuity with upstream providers in the event of provider failure?			*			
			Do you have more than one provider for each service you depend on?			*			
			Do you provide access to operational redundancy and continuity summaries, including the services you depend on?		*				
			Do you provide a tenant-triggered failover option?	*			*	*	*
			Do you share your business continuity and redundancy plans with your tenants?			*			
	Security incident management, e-discovery, & cloud forensics	Incident Response Legal Preparation	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?			*			
			Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?			*			
			Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?			*			
			Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?			*			
			Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	*			*	*	*
	Governance and Risk Management	Baseline Requirement	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?		*				*
			Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	*			*	*	*
			Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?		*		*		

Operational Requirements

Requirement	Target Verification (Control Domain)	Base Measure (Control Type)	Question	Audit Findings			Remedial Actions		
				Defective	Acceptable	Effective	Preventive	Detective	Corrective
Operational	Threat and vulnerability management	Antivirus/malicious software	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?			*			
			Do you ensure that security threat detection systems using signatures, lists, or behavioural patterns are updated across all infrastructure components within industry accepted time frames?			*			
		Vulnerability/patch management	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?			*			
			Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?			*			
			Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?			*			
			Will you make the results of vulnerability scans available to tenants at their request	*			*	*	*
			Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?			*			
	Governance and risk management	Risk assessments	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	*			*	*	*
			Do you conduct risk assessments associated with data governance requirements at least once a year?			*			
	Datacentre security	Data centre security and asset management	Do you have requirements for controlling physical access to your facility?			*			
			Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) in place?			*			
			Do you have procedures for risk assessments for physical security			*			
			Do you maintain and complete inventory of all software, network, hardware and virtual components?			*			
			Do you support asset categorisation of different sensitivity levels?						
			Do you maintain virtual segregation and physical separation of assets at different sensitivity levels?						
	Application & Interface Security	Application Security	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?			*			

			Do you use an automated source code analysis tool to detect security defects in code prior to production?		*				
			Do you use manual source-code analysis to detect security defects in code prior to production?	*			*	*	
			Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	*			*	*	
	Interoperability & Portability	APIs	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	*			*		*
		Data request	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	*					*
		Policy & Legal	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?			*			
			Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?			*			
		Standardized Network Protocols	Can data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?			*			
			Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?			*			
		Virtualisation	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?			*			
			Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review			*			
	Data Security & Information Lifecycle Management	Classification	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	*			*	*	*
			Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	*					*
			Do you have a capability to use system geographic location as an authentication factor?			*			
			Can you provide the physical location/geography of storage of a tenant's data upon request?	*					*
			Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation		*				*

Baseline Requirements

Requirement	Target Verification (Control Domain)	Base Measure (Control Type)	Question	Audit Findings			Remedial Actions		
				Defective	Acceptable	Effective	Preventive	Detective	Corrective
Baseline requirements	Datacentre security	Controlled access points	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?			*			
			Do you maintain a complete inventory of all of your critical supplier relationships?			*			
		Equipment identification	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?			*			
			Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, and replication)?	*					*
		User access	Do you restrict physical access to information assets and functions by users and support personnel?			*			
			Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?			*			
	Encryption & key mgmt.	Key generation	Do you have a capability to allow creation of unique encryption keys per tenant?			*			
			Do you have a capability to manage encryption keys on behalf of tenants?			*			
			Do you protect encryption keys, and what controls are put in place to effect that?			*			
		Storage and access	Do you have platform and data appropriate encryption that use open/validated formats and standard algorithms?		*				
			Do you have procedures in place to manage and recover compromised encryption keys?			*			
			Do you have a security policy that clearly defines what must be encrypted?		*				
	Identity & access management	Diagnostic configuration ports access	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?			*			
		User ID Credentials	Do you manage accounts with administrator or higher privileges?	*					
			Do you verify user identity and registration?			*			
			Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?			*			

			Do you use open standards to delegate authentication capabilities to your tenants?	*					*
			Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?			*			
			Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?		*				
			Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?			*			
			Do you allow tenants to use third-party identity assurance services?			*			
			Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?			*			
			Do you allow tenants/customers to define password and account lockout policies for their accounts?			*			
			Do you support the ability to force password changes upon first logon?			*			
			Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?			*			
		Source code access restriction	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?			*			
			Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?			*			
		Utility program access	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	*			*	*	
			Do you have the capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	*			*	*	
			Are attacks that target the virtual infrastructure prevented with technical controls?	*			*	*	
	Human resources	Asset returns	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	*			*	*	
			Is your Privacy Policy aligned with industry standards?			*			